



(43) 國際公開日
2004 年 10 月 21 日 (21.10.2004)

PCT

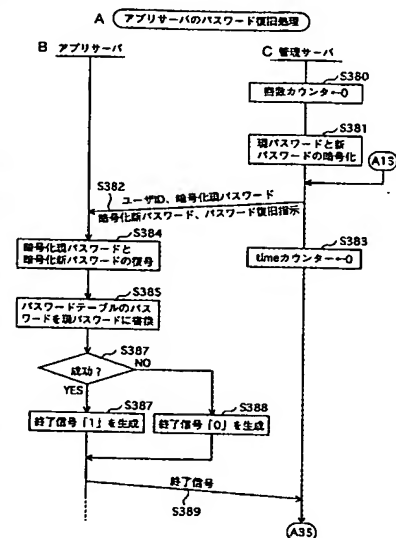
(10) 国際公開番号
WO 2004/090738 A1

- | | | | |
|-----------------------------|--|-----------------------------------|---|
| (51) 国際特許分類 ⁷ : | G06F 15/00, H04L 9/32 | (72) 発明者; および | |
| (21) 国際出願番号: | PCT/JP2004/005205 | (75) 発明者/出願人 (米国についてのみ): | 里村 尚 (SATO-MURA, Takashi). 三田村 俊朗 (MITAMURA, Toshiro). 相澤 里香 (AIZAWA, Rika). 板原 美佐紀 (ITAHARA, Misaki). |
| (22) 国際出願日: | 2004 年 4 月 12 日 (12.04.2004) | (74) 代理人: | 中島 司朗 (NAKAJIMA, Shiro); 〒5310072 大阪府大阪市北区豊崎三丁目2番1号淀川5番館6F Osaka (JP). |
| (25) 国際出願の言語: | 日本語 | (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): | AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SI, SK, SL, SM, SN, SR, ST, SV, SW, SY, TD, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VE, VN, YU, ZA, ZM, ZW. |
| (26) 国際公開の言語: | 日本語 | | |
| (30) 優先権データ: | | | |
| 特願2003-106420 | 2003 年 4 月 10 日 (10.04.2003) | JP | |
| (71) 出願人 (米国を除く全ての指定国について): | 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真1006番地 Osaka (JP). | | |

〔統葉有〕

(54) Title: PASSWORD CHANGE SYSTEM

(54) 発明の名称: パスワード変更システム



(S7) Abstract: A management server that can unify passwords for a plurality of application servers which authenticate a user by using the same password even if one of the application servers fails to change the password. If one of the application servers has failed to change the password, the management server restores the original password of an application server where the password has already been changed.

(57) 要約: 同一のパスワードにより、利用者の正当性を認証する複数のアプリサーバにおいて、複数のアプリサーバのうち何れかがパスワードの変更に失敗した場合でも、複数のアプリサーバのパスワードを統一することのできる管理サーバを提供することを目的とする。

管理サーバはパスワード変更を行う際、何れかのアプリサーバでパスワード変更が失敗した場合に、既にパスワードの変更を終えているアプリサーバのパスワードを元のパスワードに戻す。

```

A...PASSWORD RESTORATION BY APPLICATION SERVER
B...APPLICATION SERVER
C...MANAGEMENT SERVER
S380...COUNTER ← 0
S381...ENCRYPT CURRENT PASSWORD AND NEW PASSWORD
S382...SEND USER ID, ENCRYPTED CURRENT PASSWORD,
ENCRYPTED NEW PASSWORD AND ISSUE INSTRUCTION TO
RESTORE PASSWORD
S384...DECRYPT ENCRYPTED CURRENT PASSWORD AND
ENCRYPTED NEW PASSWORD
S383...time COUNTER ← 0
S385...REWRITE PASSWORD IN PASSWORD TABLE TO
CURRENT PASSWORD
S388...SUCCESSFUL?
S387...GENERATE TERMINATION SIGNAL "1"
S388...GENERATE TERMINATION SIGNAL "0"
S389...TERMINATION SIGNAL ...

```

WO 2004/090738 A1



SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US,
UZ, VC, VN, YU, ZA, ZM, ZW.

NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG,
CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(84) 指定国 (表示のない限り、全ての種類の広域保護が
可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL,
SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG,
KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY,
CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC,

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される
各PCTガゼットの巻頭に掲載されている「コードと略語
のガイダンスノート」を参照。

明 細 書
パスワード変更システム

技術分野

本発明は、パスワード変更システムに関する。

5

背景技術

従来、利用者に複数のサービスを提供する場合に、サービスを提供する各アプリケーションプログラムが、同一のパスワードを用いて、利用者の正当性を認証することが広く行われている。

- 10 このように、複数のサービスに対して同一パスワードを使用する場合において、安全性を確保するため、利用者はしばしばパスワードの変更を行う必要がある。

- 15 特許文献 1 では、同一のパスワードを用いる複数のサービスのパスワード変更方法が開示されている。このパスワード変更方法によると、パスワード管理装置は、サービスを提供する各アプリケーションプログラムを順次起動し、パスワードの変更を指示する。この際に、複数のアプリケーションプログラムのうち、何れかが正常にパスワードを変更できないという障害が発生することがある。

- 20 パスワードが正常に変更できない場合としては、例えば、システムの外部ディスクのハード障害や瞬断などの電源不良、あるいはネットワークケーブルの接続不良などの場合が有り得る。

- 25 このような障害が発生すると、パスワード管理装置は、正常にパスワード変更できないアプリケーションプログラムについては、利用者が該当するサービスを利用するためにアプリケーションプログラムを再起動したときに、利用者に再度のパスワード変更の操作を促す。

そのため、前記アプリケーションプログラムの再起動を契機として、複数のサービスに対するパスワードの整合性を維持することが可能である。

しかしながら、特許文献 1 の方法では、パスワード変更に失敗したサ

ービスのパスワードは、次にアプリケーションを起動するまで他のサービスと同一のパスワードには保たれていないという問題が発生している。

特許文献 1 特開 2002 - 169777 号公報

発明の開示

5 そこで本発明はかかる問題点に鑑みてなされたものであり、複数のアプリケーション装置のうち何れかがパスワードの変更に失敗した場合でも、複数のアプリケーション装置のパスワードを統一することのできる管理サーバ装置、アプリケーション装置、パスワード変更システムを提供することを目的とする。

10 上記目的を達成するために本発明は、一のパスワードにより認証した一の利用者へ各サービスを提供する複数のアプリケーション装置に対して、当該パスワードの更新を指示する管理サーバ装置であって、全てのアプリケーション装置のパスワードの更新を試みる第 1 手段と、各アプリケーション装置について、パスワードの更新が不可能か否かを判断する
15 第 2 手段と、不可能と判断されるアプリケーション装置が少なくとも 1 台存在する場合に、全てのアプリケーション装置のパスワードを更新前のものとする第 3 手段とを備える。

20 この構成によると、前記第 2 手段によりパスワードの更新が不可能であると判断されるアプリケーション装置が存在すると判断される場合でも、全てのアプリケーション装置のパスワードを更新前のものとする
20 ことで、複数のアプリケーション装置のパスワードの統一を保つことができる。

25 前記管理サーバ装置は、さらに、利用者装置からパスワードの更新の要求を受信する第 4 手段を含み、前記第 1 手段は、受信した前記更新の要求に基づいて、パスワードの更新を試みるとしてもよい。

30 この構成により、前記管理サーバ装置は、利用者の意思に基づきパスワードの更新を試みることができる。

35 また、前記管理サーバ装置において、前記第 1 手段は、全てのアプリケーション装置に対してパスワードの更新を指示し、前記第 2 手段は、

各アプリケーション装置について、パスワードの更新が失敗したか否かを判断し、前記第3手段は、少なくとも1台のアプリケーション装置について、更新が失敗したと判断される場合に、パスワードの更新が成功した他のアプリケーション装置に対して、更新前のパスワードへの復元を指示する。

これによると、前記第2判断手段は、何れかのアプリケーション装置のパスワード更新が失敗したか否かを判断し、前記第3判断手段は、少なくとも1台のアプリケーション装置のパスワード更新が失敗したと判断される場合に、パスワード更新が成功したアプリケーション装置に対し、更新前のパスワードへの復元を指示するので、前記アプリケーション装置のうち何れかが、パスワードの更新に失敗した場合にも、全てのアプリケーション装置のパスワードを速やかに統一することができる。

本発明において、前記第4手段は、利用者の新パスワードと旧パスワードとを含む前記更新の要求を受信し、前記第1手段は、受信した更新の要求に含まれる新パスワードと旧パスワードとを含む更新の指示を生成し、生成した前記更新の指示を全てのアプリケーション装置に対して送信することを特徴とする。

この構成によると、前記第4手段は利用者から前記新パスワードを含む前記パスワード更新の指示を受け付ける。これにより、利用者自身が任意の新パスワードを指定することができる。

また、本発明において、前記第2手段は、各アプリケーション装置からのパスワードの更新の成功又は失敗を示す応答を受信する応答受信部と、受信した前記応答が成功を示す場合に、当該アプリケーション装置についてパスワードの更新が成功したと断定し、受信した前記応答が失敗を示す場合に、当該アプリケーション装置についてパスワードの更新が失敗したと断定する断定部とを含むことを特徴とする。

この構成によると、前記応答受信部は、各アプリケーション装置からの応答を受信し、前記判断部は、前記応答が失敗を示す場合にアプリケーション装置のパスワード変更が失敗であると断定する。これにより、

各アプリケーション装置のパスワード更新の失敗を正確に検出することができる。

また、本発明は、前記第2手段が、時間の経過に伴って経過時間を計測する計時部と、前記第1手段による更新の指示の送信の時点において、
5 計時部により計測される経過時間を初期値にリセットする初期化部と、各アプリケーション装置からのパスワードの更新の成功又は失敗を示す応答を待ち受ける待受部と、計測された経過時間が、所定のしきい値より大きいか否かを判断する判断部と、判断部により経過時間が前記しきい値と等しいか又は小さいと判断され、かつ待受部により各アプリケーション装置からの応答を受信し、かつその応答が成功を示す場合に、当
10 該アプリケーション装置について、パスワードの更新が成功したと断定し、その他の場合に、当該アプリケーション装置について、パスワードの更新が失敗したと断定する断定部とを含むことを特徴とする管理サーバ装置である。

15 この構成によると、前記断定部は、前記閾値を超えても、前記応答を受信しない場合をパスワード変更の失敗と断定する、このため、前記閾値以上の無駄な待ち時間を削減できる。

本発明は、前記第1手段は、全てのアプリケーション装置に対してパスワードの更新の準備を指示し、前記第2手段は、各アプリケーション装置について、パスワードの更新の準備が未完了か否かを判断し、前記
20 第3手段は、少なくとも1台のアプリケーション装置について、更新の準備が未完了と判断される場合に、更新の準備が完了した他のアプリケーション装置に対して、前記更新の準備の指示を取り消すことを特徴とする管理サーバ装置でもある。

25 この構成によると、パスワード更新の準備が未完了のアプリケーション装置が1つでも存在すると、前記パスワード更新の準備が完了したアプリケーション装置のパスワード更新の準備を取り消す。これにより、全てのアプリケーション装置のパスワード更新の準備が完了するまで、各アプリケーション装置のパスワード更新は実行されないため、ハード

ディスクへの無駄な書き込みを回避できる。

本発明において、前記第4手段は、利用者の新パスワードと旧パスワードとを含む前記更新の要求を受信し、前記第1手段は、受信した更新の要求に含まれる新パスワードと旧パスワードとを含む更新の準備の指示を生成し、生成した前記更新の準備の指示を全てのアプリケーション装置に対して送信することを特徴とする。

この構成によると、前記第4手段は利用者から前記新パスワードを含む前記パスワード更新の指示を受け付ける。これにより、利用者自身が任意の新パスワードを指定することができる。

また、本発明の管理サーバ装置において、前記第2手段は、アプリケーション装置からのパスワードの更新の準備の完了又は未完了を示す応答を受信する応答受信部と、受信した前記応答が完了を示す場合に、当該アプリケーション装置についてパスワードの更新の準備が完了したと断定し、受信した前記応答が未完了を示す場合に、当該アプリケーション装置についてパスワードの更新の準備が未完了であると断定する断定部とを含むことを特徴とする。

この構成によると、前記応答受信部は、各アプリケーション装置からの応答を受信し、前記判断部は、前記応答が未完了を示す場合にアプリケーション装置のパスワード変更準備が未完了であると断定する。これにより、各アプリケーション装置のパスワード更新準備の未完了を正確に検出することができる。

本発明において、前記第2手段は、時間の経過に伴って経過時間を計測する計時部と、前記第1手段による更新の準備の指示の送信の時点において、計時部により計測される経過時間を初期値にリセットする初期化部と、アプリケーション装置からのパスワードの更新の準備の完了又は未完了を示す応答を待ち受ける待受部と、計測された経過時間が、所定のしきい値より大きいか否かを判断する判断部と、判断部により経過時間が前記しきい値と等しいか又は小さいと判断され、かつ待受部によりアプリケーション装置からの応答を受信し、かつその応答が完了を示

す場合に、パスワードの更新の準備が完了したと断定し、その他の場合に、パスワードの更新の準備が未完了であると断定する断定部とを含むことを特徴とする。

- この構成によると、前記閾値を超えても、前記応答を受信しない場合
5 をパスワード変更の失敗と断定することにより、前記閾値以上の無駄な待ち時間を削減できる。

- 本発明である前記管理サーバ装置は、さらに、前記第2手段によりパスワードの更新が不可能と判断される場合に、元のパスワードに戻す旨のメッセージを前記利用者装置へ送信するメッセージ送信手段を含むこと
10 を特徴とする。

この構成によると、前記メッセージ送信手段は、前記利用者装置へ前記メッセージを送信するため、利用者は、使用すべきパスワードが更新前のものであることを知ることができる。

- 前記管理サーバ装置は、さらに、各アプリケーション装置について、
15 メインテナンス中であるか否かを記憶している管理記憶手段を備え、前記第1手段は、メインテナンス中のアプリケーション装置が存在しない場合に、パスワードの更新を試みることを特徴とする。

- この構成によると、前記第1手段は、メインテナンス中のアプリケーション装置が存在しない場合にパスワード更新を試みるため、メイン
20 テナンス中のアプリケーション装置のパスワード更新により、その他のアプリケーション装置のパスワード変更が妨げられることを予め回避することができる。

- また、前記第1手段は、メインテナンス中のアプリケーション装置が存在する場合に、パスワードの更新を中止し、前記管理サーバ装置は、
25 さらに、前記第1手段によりパスワードの更新が中止される場合に、パスワードの更新を中止する旨のメッセージを前記利用者装置へ送信するメッセージ送信手段を含むことを特徴とする。

この構成によると、前記メッセージ送信手段は、前記利用者装置へパスワードの更新を中断する旨のメッセージを送信するので、利用者は、

パスワード更新ができないことを確実に知ることができる。

- また、本発明において、前記アプリケーション装置は、第1ネットワークを介して、前記管理サーバ装置と接続されており、前記利用者装置は、第1ネットワークに接続されていない第2ネットワークを介して、
- 5 前記管理サーバ装置と接続されていることを特徴とする。

この構成によると、前記アプリケーション装置と前記利用者装置は、前記管理サーバ装置を介して接続されているため、前記管理サーバ装置は、前記アプリケーション装置と前記利用者装置の間の通信を監視することができる。

- 10 本発明において、前記第1ネットワーク及び前記第2ネットワークは、イントラネットであることを特徴とする。

- この構成によると、前記アプリケーション装置と前記利用者装置とはそれぞれ異なるイントラネットを介して、管理サーバ装置と接続されているため、インターネットで普及している技術を利用して、容易に構成
- 15 できる。

- また、本発明において、前記管理サーバ装置と、各アプリケーション装置とは、専用線を介して、接続されており、パスワードの更新の際には、前記管理サーバ装置は、前記専用線を介して、各アプリケーション装置との間で、パスワードの更新のための情報を送受信し、各サービスの提供の際には、前記管理サーバ装置は、第1及び第2ネットワークを
- 20 介して、前記利用者装置と各アプリケーション装置との間で、前記サービスに係る情報の送受信を中継するとしてもよい。

- この構成によると、前記管理サーバ装置は、パスワードの更新の際には、前記専用線を介して、各アプリケーション装置との間で、パスワードの更新のための情報を送受信する。専用線によりる通信は、第三者による盗聴の危険性が少ないので、パスワード更新の際の情報の送受信の暗号化の処理を省略することができる。
- 25

また、各サービスの提供の際には、前記管理サーバ装置は、第1及び第2ネットワークを介して、前記利用者装置と各アプリケーション装置

との間で、前記サービスに係る情報の送受信を中継するため、パスワード更新のための情報の送受信と前記サービスに係る情報の送受信は互いに影響を及ぼすことがない。

5 また、本発明における前記アプリケーション装置及び前記利用者装置は、ネットワークを介して、前記管理サーバ装置と接続されており、前記管理サーバ装置は、さらに、アプリケーションの種類と、各アプリケーション装置のネットワーク上における位置情報とを対応付ける対応テーブルを記憶している記憶手段と、前記利用者装置から、アプリケーションを示す種類情報と処理の内容を示す処理情報とを受信する受信手段と、前記対応テーブルを用いて、受信した種類情報に対応するアプリケーション装置の位置情報を取得する取得手段と、取得した位置情報により示されるアプリケーション装置に対して、前記処理情報を送信する送信手段とを含むとしてもよい。

15 この構成によると、前記取得手段は前記対応テーブルを用いて前記種類情報に対応するアプリケーション装置の位置情報を取得し、前記送信手段は、前記位置情報により示されるアプリケーション装置に対して、前記利用者装置から受信した前記処理情報を送信する。これにより、前記管理サーバ装置は、前記利用者装置から送信された処理情報をアプリケーション装置へ正確に転送できる。

20 また、前記ネットワークは、インターネットであるとしてもよい。

 この構成によると、前記管理サーバ装置は、インターネットを介して遠隔地に存在する利用者装置と各アプリケーション装置との間で前記処理情報を転送することができる。

25 本発明は、更新後の新パスワードが、利用者に最初に割り当てられた初期パスワードであり、前記第1手段は、全てのアプリケーション装置の初期パスワードへの更新を試み、前記第2手段は、各アプリケーション装置について、初期パスワードへの更新が不可能か否かを判断し、前記第3手段は、不可能と判断されるアプリケーション装置が少なくとも1台存在する場合に、全てのアプリケーション装置のパスワードを更新

前のものとすることを特徴とする管理サーバ装置でもある。

この構成によると、前記第 1 手段は、前記初期パスワードへの更新を試みる。これにより、利用者による新パスワードの指定ができない場合でも、パスワードの更新を試みることができる。

- 5 本発明は、一のパスワードにより認証した一の利用者へサービスを提供し、管理サーバ装置からの指示によりパスワードを更新するアプリケーション装置であって、更新前のパスワードを記憶している旧パスワード記憶手段と、利用者の認証に用いるパスワードを記憶している認証用パスワード記憶手段と、管理サーバ装置から、パスワードを更新前のものに復元する復元指示を受信する受信手段と、前記復元指示を受信すると、旧パスワード記憶手段から更新前のパスワードを読み出し、読み出したパスワードを認証用パスワード記憶手段に上書きする書込手段とを備えることを特徴とするアプリケーション装置である。
- 10

- この構成によると、管理サーバ装置から復元指示を受信すると、旧パスワード記憶手段の記憶している旧パスワード記憶手段から更新前のパスワードを読み出し、読み出したパスワードを認証用パスワード記憶手段に上書きするため、管理サーバ装置の指示により、認証用のパスワードを更新前のパスワードに速やかに変更することができる。
- 15

- また、前記アプリケーション装置は、前記管理サーバ装置を介して、利用者の利用者装置との間で、前記サービスに関する情報の送受信を行うことを特徴とする。
- 20

- この構成によると、前記アプリケーション装置は、前記管理サーバ装置を介して利用者端末との間で、情報の送受信を行うため、前記管理サーバ装置以外からの情報の受信を拒否することで、正当な利用者以外からのアクセスを回避できる。
- 25

本発明のアプリケーション装置は、メンテナンス中である場合に、当該旨を前記管理サーバ装置に対して通知することを特徴とする。

この構成によると、前記アプリケーション装置は、メンテナンス中である旨をあらかじめ管理サーバ装置へ通知しているので、前記管理サ

サーバ装置は、前記アプリケーション装置がメンテナンス中であることを事前に認識しており、当該アプリケーション装置に対する情報の送信及び指示の送信を中止又は延期することができる。

5 前記アプリケーション装置は、第1ネットワークを介して、前記管理サーバ装置と接続されており、前記利用者装置は、第1ネットワークに接続されていない第2ネットワークを介して、前記管理サーバ装置と接続されていることを特徴とする。

10 この構成によると、前記アプリケーション装置と前記利用者装置は、前記管理サーバ装置を介して接続されているため、前記管理サーバ装置は、前記アプリケーション装置と前記利用者装置の間の通信を監視することができる。

15 また、前記アプリケーション装置及び前記管理サーバ装置は、専用線を介して接続されており、パスワードの更新の際には、前記管理サーバ装置は、前記専用線を介して、前記管理サーバとの間で、パスワードの更新のための情報を送受信し、各サービスの提供の際には、第1及び第2ネットワークを介して、前記サービスに係る情報を送受信することを特徴とするとしてもよい。

20 この構成によると、前記アプリケーション装置は、パスワード更新に関する情報の送受信には前記専用線を使用するため、第三者による盗聴が行われにくく、通信の安全性が高い。

また、各サービスに係る情報の送受信には第1ネットワーク及び第2ネットワークを使用するため、パスワード更新に関する情報の送受信とサービスに係る情報の送受信とは互いに影響を及ぼさない。

25 また、本発明における前記アプリケーション装置及び前記利用者装置は、インターネットを介して、前記管理サーバ装置と接続されていることを特徴とする。

この構成によると、前記アプリケーション装置及び前記利用者装置はインターネットを介して前記管理サーバ装置に接続されているため、前記アプリケーション装置、前記利用者装置及び前記管理サーバ装置がそ

れぞれ遠隔地に存在している場合でも、情報の送受信を行うことができる。

5 本発明は、利用者の端末装置と、一のパスワードにより認証した一の利用者の端末装置へ各サービスを提供する複数のアプリケーション装置と、前記アプリケーション装置に対して、当該パスワードの更新を指示する管理サーバ装置とから構成されるパスワード更新システムであって、前記管理サーバ装置は、全てのアプリケーション装置のパスワードの更新を試みる第1手段と、各アプリケーション装置について、パスワードの更新が不可能か否かを判断する第2手段と、不可能と判断されるアプリケーション装置が少なくとも1台存在する場合に、全てのアプリケーション装置のパスワードを更新前のものとする第3手段とを備え、各アプリケーション装置は、更新前のパスワードを記憶している旧パスワード記憶手段と、利用者の認証に用いるパスワードを記憶している認証用パスワード記憶手段と、管理サーバ装置から、パスワードを更新前のものに復元する復元指示を受信する受信手段と、前記復元指示を受信すると、旧パスワード記憶手段から更新前のパスワードを読み出し、読み出したパスワードを認証用パスワード記憶手段に上書きする書込手段とを備えることを特徴とする。

20 この構成により、複数のアプリケーション装置のうち何れかがパスワード更新不可能と判断される場合においても、全てのアプリケーション装置のパスワードを更新前のものとするにより、全てのアプリケーション装置のパスワードの統一を保つことができる。

本発明における前記端末装置と各アプリケーション装置とは、前記管理サーバ装置を介して、情報の送受信を行うことを特徴とする。

25 この構成によると、前記アプリケーション装置は、前記管理サーバ装置を介して利用者端末との間で、情報の送受信を行うため、前記管理サーバ装置以外からの情報の受信を拒否することで、正当な利用者以外からのアクセスを回避できる。

また、前記アプリケーション装置は、第1ネットワークを介して、前

記管理サーバ装置と接続されており、前記利用者装置は、第1ネットワークに接続されていない第2ネットワークを介して、前記管理サーバ装置と接続されていることを特徴とする。

- 5 この構成によると、前記アプリケーション装置と前記利用者装置は、前記管理サーバ装置を介して接続されているため、前記管理サーバ装置は、前記アプリケーション装置と前記利用者装置の間の通信を監視することができる。

また、前記パスワード更新システムにおいて、前記第1ネットワーク及び前記第2ネットワークは、イントラネットであることを特徴とする。

- 10 この構成によると、前記アプリケーション装置と前記利用者装置とはそれぞれ異なるイントラネットを介して、管理サーバ装置と接続されているため、インターネットで普及している技術を利用して、容易に構成できる。

- 15 前記パスワード更新システムにおいて、前記管理サーバ装置と、各アプリケーション装置とは、専用回線を介して、接続されており、パスワードの更新の際には、前記管理サーバ装置は、前記専用線を介して、前記管理サーバとの間で、パスワードの更新のための情報を送受信し、各サービスの提供の際には、第1及び第2ネットワークを介して、前記サービスに係る情報を送受信するとしてもよい。

- 20 この構成によると、前記アプリケーション装置は、パスワード更新に関する情報の送受信には前記専用線を使用するため、第三者による盗聴が行われにくく、通信の安全性が高い。

- 25 また、各サービスに係る情報の送受信には第1ネットワーク及び第2ネットワークを使用するため、パスワード更新に関する情報の送受信とサービスに係る情報の送受信とは互いに影響を及ぼさない。

本発明のパスワード更新システムは、前記アプリケーション装置及び前記利用者装置は、ネットワークを介して、前記管理サーバ装置と接続されており、前記管理サーバ装置は、さらに、アプリケーションの種類と、各アプリケーション装置のネットワーク上における位置情報とを対

応付ける対応テーブルを記憶している記憶手段と、前記利用者装置から、アプリケーションを示す種類情報と処理の内容を示す処理情報とを受信する受信手段と、前記対応テーブルを用いて、受信した種類情報に対応するアプリケーション装置の位置情報を取得する取得手段と、取得した位置情報により示されるアプリケーション装置に対して、前記処理情報を送信する送信手段とを含むことを特徴とするとしてもよい。

この構成によると、前記取得手段は前記対応テーブルを用いて前記種類情報に対応するアプリケーション装置の位置情報を取得し、前記送信手段は、前記位置情報により示されるアプリケーション装置に対して、前記利用者装置から受信した前記処理情報を送信する。これにより、前記管理サーバ装置は、前記利用者装置から送信された処理情報をアプリケーション装置へ正確に転送できる。

また、前記ネットワークは、インターネットであることを特徴とする。

この構成によると、前記アプリケーション装置及び前記利用者装置はインターネットを介して前記管理サーバ装置に接続されているため、前記アプリケーション装置、前記利用者装置及び前記管理サーバ装置がそれぞれ遠隔地に存在している場合でも、情報の送受信を行うことができる。

図面の簡単な説明

図 1 は、パスワード変更システムの構成図である。

図 2 は、ユーザ端末 100 の構成を示すブロック図である。

図 3 は、記憶部 110 に記憶されている情報の一例を示す。

図 4 は、本実施の形態で、各機器間で送受信される情報の形態を示す。

図 5 は、ユーザ端末 100 に接続されているモニタに表示されるログイン画面とメニュー画面の一例を示す。

図 6 は、ユーザ端末 100 に接続されているモニタに表示される精算画面と精算終了画面の一例を示す。

図 7 は、ユーザ端末 100 に接続されているモニタに表示されるパスワード変更画面と変更完了画面の一例を示す。

図 8 は、ユーザ端末 1 0 0 に接続されているモニタに表示される変更失敗画面と強制終了画面の一例を示す。

図 9 は、アプリサーバ 2 0 0 の構成を示すブロック図である。

図 1 0 は、情報記憶部 2 1 0 に記憶されている情報の一例である。

5 図 1 1 は、パスワードテーブル 2 2 1 の詳細を示している。

図 1 2 は、アプリログインテーブル 2 3 1 の詳細を示している。

図 1 3 は、管理サーバ 6 0 0 の構成を示すブロック図である。

図 1 4 は、情報記憶部 6 1 0 に記憶されている情報の一例を示す。

図 1 5 は、ログインテーブル 6 3 1 の詳細を示す。

10 図 1 6 は、ルーティングテーブル 6 4 1 の詳細を示す。

図 1 7 は、パスワード変更テーブル 6 5 1 の詳細を示す。

図 1 8 は、管理サーバ 6 0 0 の表示部 6 1 3 に表示されるエラー画面の一例である。

15 図 1 9 は、ユーザ端末 1 0 0、管理サーバ 6 0 0 及びアプリサーバ 2 0 0 による動作を示したフローチャートである。

図 2 0 は、ユーザ端末 1 0 0、管理サーバ 6 0 0 及びアプリサーバ 2 0 0 による動作を示したフローチャートである。図 1 9 より続く。

図 2 1 は、ユーザ端末 1 0 0、管理サーバ 6 0 0 及びアプリサーバ 2 0 0 による動作を示したフローチャートである。図 1 9 より続く。

20 図 2 2 は、ユーザ端末 1 0 0、管理サーバ 6 0 0 及びアプリサーバ 2 0 0 による動作を示したフローチャートである。図 1 9 より続く。

図 2 3 は、ユーザ端末 1 0 0、管理サーバ 6 0 0 及びアプリサーバ 2 0 0 による動作を示したフローチャートである。図 1 9 より続く。

25 図 2 4 は、ユーザ端末 1 0 0、管理サーバ 6 0 0 及びアプリサーバ 2 0 0 による動作を示したフローチャートである。図 1 9 より続く。

図 2 5 は、ユーザ端末 1 0 0、管理サーバ 6 0 0 及びアプリサーバ 2 0 0 による動作を示したフローチャートである。図 1 9 より続く。

図 2 6 は、ユーザ端末 1 0 0、管理サーバ 6 0 0 及びアプリサーバ 2 0 0 による動作を示したフローチャートである。図 1 9 より続く。

図 27 は、管理サーバ 600 によるパスワード変更処理の動作を示すフローチャートである。

図 28 は、管理サーバ 600 によるパスワード変更処理の動作を示すフローチャートである。図 27 より続く。

- 5 図 29 は、管理サーバ 600 によるパスワード変更処理の動作を示すフローチャートである。図 27 より続く。

図 30 は、アプリサーバ 200 のパスワード変更処理の動作を示すフローチャートである。

- 10 図 31 は、アプリサーバ 200 のパスワード変更処理の動作を示すフローチャートである。図 30 より続く。

図 32 は、管理サーバ 600 によるパスワード復旧の動作を示すフローチャートである。

図 33 は、アプリサーバ 200 のパスワード復旧の動作を示すフローチャートである。

- 15 図 34 は、アプリサーバ 200 のパスワード復旧の動作を示すフローチャートである。図 33 より続く。

図 35 は、二つの機器間の相互認証の動作を示したフローチャートである。

- 20 図 36 は、二つの機器間の相互認証の動作を示したフローチャートである。図 35 より続く。

図 37 は、実施の形態 1 における、パスワード変更の実行中の各アプリサーバ 200 の記憶しているパスワードを示している。

図 38 は、実施の形態 2 の構成を示した構成図である。

- 25 図 39 は、実施の形態 2 における管理サーバ 600 b の構成を示すブロック図である。

図 40 は、実施の形態 3 の構成を示した構成図である。

図 41 は、実施の形態 2 における管理サーバ 600 c の構成を示すブロック図である。

図 42 は、変形例 (1) におけるパスワードテーブル 621 b の詳細を

示す。

図43は、変形例(6)におけるルーティングテーブル641bの詳細を示す。

発明を実施するための最良の形態

5 1. 実施の形態1

以下、本発明の実施の形態1について図面を用いて詳細に説明する。

1. 1パスワード変更システムの概要

本発明におけるパスワード変更システムは、図1に示すように、ユーザ端末100、第1アプリサーバ200a、第2アプリサーバ200b、
10 第3アプリサーバ200c、第4アプリサーバ200d及び管理サーバ600から構成される。各装置は、インターネット20に接続されている。

第1アプリサーバ200a～第4アプリサーバ200dは、それぞれ、出張費精算、休暇申請、会議室予約、従業員購入のサービスを提供する。

15 管理サーバ600及び第1アプリサーバ200a～第4アプリサーバ200dは、あらかじめ正当な利用者のユーザIDとを記憶している。

利用者は、ユーザ端末100を用いて、インターネット20と管理サーバ600とを介して、第1アプリサーバ200a～第4アプリサーバ200dの提供するサービスを利用する。

20 このとき、ユーザ端末100は、管理サーバ600に利用者のユーザIDとパスワードを送信する。

管理サーバ600及び第1アプリサーバ200a～第4アプリサーバ200dは、ユーザIDとパスワードを検証し、ユーザ端末100の利用者が正当な利用者であることを認証し、各アプリサーバは、それぞれ
25 が備えるサービスを提供する。

また、管理サーバ600は、ユーザ端末100からパスワード変更の指示を受信し、ユーザ端末100から、現在のパスワードと新しいパスワードとを受信する。管理サーバ600は、第1アプリサーバ200a～第4アプリサーバ200dへ、受け取った新しいパスワードを順次送

信し、パスワードの変更を指示する。

ここで、第1アプリサーバ200a～第4アプリサーバ200dの何れかで、パスワードの変更が正常に行われなかった場合、管理サーバ600は、既にパスワード変更が終了しているアプリサーバに現在のパスワードを送信し、現在のパスワードへパスワードを変更し直すように指示する。

以下の説明において第1アプリサーバ200a～第4アプリサーバ200dを特に区別しない場合及び第1アプリサーバ200a～第4アプリサーバ200d全てに共通する場合、これらを単にアプリサーバ200と呼称する。

1. 2 ユーザ端末100

ユーザ端末100は、図2に示すように、送受信部101、認証部103、制御部107、記憶部110、入力部112及び画像表示部113から構成される。

ユーザ端末100は、具体的には図示されていないマイクロプロセッサ、RAM、ROM及びハードディスクから構成されている。前記RAM、ROM及びハードディスクにはコンピュータプログラムが記憶されており、前記マイクロプロセッサがこれらのコンピュータプログラムに従って動作することにより、ユーザ端末100はその機能を果たす。

20 (1) 記憶部110

記憶部110は、ハードディスク、RAM及びROMから構成され、各種情報を記憶している。

一例として、図3に示すように、アプリ番号表120、端末ID130、秘密鍵135、公開鍵証明書136、CRL (Certificate Revocation List) 137及び認証局公開鍵138を記憶している。

アプリ番号表120は、アプリサーバ200及び管理サーバ600の提供するサービスと各サービスに割り当てられたアプリ番号とを対応付ける表である。アプリ番号「001」は、出張費精算サービスを示す識

別番号であり、アプリ番号「002」は休暇申請サービスを示す識別番号である。アプリ番号「003」は、会議室予約サービスを示す識別番号であり、アプリ番号「004」は、従業員購入サービスを示す識別番号である。アプリ番号「005」は、ログイン処理、パスワードの変更
5 など管理サーバの提供するサービスを示す識別番号である。

端末ID130は、ユーザ端末100に固有の識別情報である。

公開鍵証明書136は、秘密鍵135と対になる公開鍵の正当性を証明するものであり、証明書ID、前記公開鍵及び認証局による署名データを含む。認証局の署名データは、認証局の秘密鍵を用いて、前記公開
10 鍵に署名生成アルゴリズムSを施して、生成したものである。ここで、認証局は、第三者機関であり、パスワード変更システムに属する各機器の公開鍵証明書を発行する。なお、署名生成アルゴリズムSは一例として、有限体上のElGamal署名である。ElGamal署名については、公知であるので説明を省略する。

15 CRL137は、認証局により発行され、無効になった公開鍵証明書の証明書IDを含む。

認証局公開鍵138は、認証局の秘密鍵と対になる公開鍵である。

(2) 送受信部101

送受信部101は、インターネット20に接続されている外部機器と
20 制御部107及び認証部103の間で情報の送受信を行う。

送受信部101は、ユーザ端末100及び管理サーバ600のIPアドレスを記憶している。

送受信部101が送受信する各種の情報は、図4に示すパケット140のような形体である。パケット140は、送信先アドレス141、送信元アドレス142及びデータ部143から構成される。送信先アドレスは、送信先のIPアドレス、送信元アドレス142は、送信元のIP
25 アドレスである。データ部143は、一例として、アプリ番号146、端末ID147及びデータ148を含む。

アプリ番号146は、第1アプリサーバ200a～第4アプリサーバ

及び管理サーバ600の提供するサービスの種類と対応しており、これは、アプリ番号表120に含まれるアプリ番号と同一である。

5 送受信部101は、制御部107から、アプリ番号146、端末ID147及びデータ148からなるデータ部143を受け取り送信の指示を受けると、受け取ったデータ部143に送信元アドレスとしてユーザ端末100のIPアドレスを設定し、送信先アドレスとして管理サーバ600のIPアドレスを設定して送信する。

10 ここでは、説明を容易にするために、データ部143に含まれるアプリ番号146、端末ID147及びデータ148を列挙しているが、実際には、データ部143は、可変長であるが最大ビット長が決まっているため、データ部143が最大ビット長を超える場合は、データ部143を分割し、分割されたデータ部143それぞれに、送信先アドレスと送信元アドレスとを設定し、送信する。

(3) 入力部112

15 入力部112は、キーボード、マウスといった周辺機器と接続されており、利用者による周辺機器の操作を受け付け、受け付けた操作に応じた操作指示情報を制御部107へ出力する。

(4) 制御部107

20 制御部107は、上記のプロセッサがコンピュータプログラムに従って動作することにより、ユーザ端末100で実行する各種の情報処理を制御する。

本願に関しては、制御部107は、入力部112から各種の操作指示情報を受け取る。受け取った操作指示情報により、ログイン処理、各種サービスの利用及びパスワードの変更処理等を行う。

25 また、これらの処理の途中で、管理サーバ600からログイン画面データ、端末用メニュー画面データ、端末用精算画面データ、端末用精算完了画面データ、端末用パスワード変更画面データ、端末用変更完了画面データ、端末用変更失敗画面データ、端末用強制終了画面データ等の画面データ、各種サービス、パスワード変更、相互認証、暗号処理に関

する各種情報を受信し、受信した各種画面データ及び各種の情報を処理する。

上記の処理中に、制御部 107 が送受信部 101 を介して管理サーバ 600 へ送信する情報は、図 4 に示すパケット 140 の形体をしている。

- 5 制御部 107 は、記憶部 110 から端末 ID 130 を読み出し、アプリ番号表 120 からアプリ番号を抽出し、読み出した端末 ID 130 と抽出したアプリ番号と各種情報からなるデータ部 143 を生成する。生成したデータ部 143 を送受信部 101 へ出力し、送信を指示する。

- 10 以下の説明において、データ部 143 の生成についての説明は簡略化し、単にアプリ番号と端末 ID と各種情報と表現する。

以下に、ログイン処理、各種サービスの利用の処理及びパスワードの変更処理について、説明する。

(ログイン処理)

- 15 制御部 107 は、入力部 112 から、電子申請を示す操作指示情報を受け取ると、認証部 103 へ、管理サーバ 600 との間の相互認証を指示する。

- 20 認証部 103 による相互認証が成立し、認証部 103 から、端末共通鍵を受け取り、受け取った端末共通鍵を記憶する。次に、送受信部 101 を介して、管理サーバ 600 から、ログイン画面データを受信し、受信したログイン画面データからログイン画面 151 を生成し、生成したログイン画面 151 を画像表示部 113 へ出力し、ログイン画面 151 の表示を指示する。図 5 に示すログイン画面 151 は、ここで表示される画面の一例である。ログイン画面データは、ログイン画面 151 を生成するためのデータであり HTML により記述される。

- 25 次に、入力部 112 を介して利用者の入力及びを受け付ける。送信ボタン 154 の押下を示す操作指示情報を受け取ると、パスワードボックス 153 に記入されたパスワードと端末共通鍵とを暗号処理部 108 へ出力し、暗号化を指示する。次に、暗号処理部 108 から暗号化パスワードを受け取り、記憶部 110 からアプリ番号「005」と端末 ID 1

30とを読み出す。読み出したアプリ番号「005」と端末ID130と受け取った暗号化パスワードとユーザIDボックス152に入力されたユーザIDとを送受信部101へ出力し、管理サーバ600への送信を指示する。

5 (各種サービスの利用)

次に、管理サーバ600から、端末用メニュー画面データを受信し、受信した端末用メニュー画面データからメニュー画面161を生成し、生成したメニュー画面161を画像表示部113に出力し、メニュー画面161の表示を指示する。図5は、ここで表示される示すメニュー画面161の一例である。端末用メニュー画面データは、メニュー画面161を生成するためのデータであり、HTMLにより記述される。

次に、入力部112から、メニュー画面161上に表示されるボタン162～166の押下を示す操作指示情報を受け取る。

制御部107は、入力部112からボタン162、163、164又は165の押下を示す操作指示情報を受け取り、それぞれ、出張費精算、休暇申請、会議室予約又は従業員購入のサービスの利用の処理を開始する。

ここでは、一例として、出張費精算サービスの利用についてのみ、具体的に説明する。

20 ボタン162の押下を示す操作指示情報を入力部112から受け取ると、制御部107は、記憶部110のアプリ番号表120から、アプリ番号「001」を抽出し、端末ID130を読み出し、抽出したアプリ番号「001」と読み出した端末ID130とを送受信部101を介して管理サーバ600へ送信し、サービス開始を要求する。

25 次に、制御部107は、送受信部101を介して、管理サーバ600から、waitメッセージ、端末用強制終了画面データ又は端末用精算画面データを受信する。端末用強制終了画面データ及び端末用精算画面データは、強制終了画面321及び精算画面171を生成するためのデータでありHTMLにより記述される。

waitメッセージを受信すると、画像表示部113を介して受信したwaitメッセージをモニタに表示し、次に、画像表示部113を介してメニュー画面161をモニタに表示し、メニューの選択の受付から処理をやり直す。

- 5 端末用強制終了画面データを受信すると、受信した端末用強制終了画面データから強制終了画面321を生成し、生成した強制終了画面321を画像表示部113へ出力し、強制終了画面321の表示を指示し、処理を終了する。図8に示す強制終了画面321は、ここで表示される画面の一例である。

- 10 端末用精算画面データを受け取ると、受け取った端末用精算画面データから精算画面171を生成し、生成した精算画面171画像表示部113へ出力し、精算画面171の表示を指示する。図6は、ここで表示される精算画面171の一例である。

- 次に、入力部112を介して利用者による入力を受け付ける。入力部112から、精算画面171上の送信ボタン173の押下を示す操作指示情報を受け取り、精算画面171上に入力されている入力データと端末共通鍵とを暗号処理部108へ出力し、暗号化を指示する。図4に示すデータ149はここで出力される入力データの一例であり、行き先、交通機関名、料金などを含む。

- 20 暗号処理部108から暗号化入力データを受け取り、記憶部110からアプリ番号「001」と端末ID130とを読み出し、読み出したアプリ番号「001」と端末ID130と受け取った暗号化入力データとを、送受信部101を介して管理サーバ600へ送信する。

- 次に、管理サーバ600から、端末用精算終了画面データを受信し、25 受信した端末用精算終了画面データから精算終了画面181を生成し、生成した精算終了画面181を画像表示部113へ出力し、表示を指示する。図6に示す精算終了画面181は、ここで表示される画面の一例である。端末用精算終了画面データは、精算終了画面を生成するためのデータであり、HTMLにより記述される。

次に、入力部 112 から、精算終了画面 181 上のメニューボタン 182 又はログアウトボタン 183 の押下を示す操作指示情報を受け取る。

メニューボタン 182 の押下を示す操作指示情報を受け取ると、画像表示部 113 にメニュー画面 161 の表示を指示し、メニューの選択を受け付ける。

ログアウトボタン 183 の押下を示す操作指示情報を受け取ると、制御部 107 は、ログアウト通知を生成し、記憶部 110 からアプリ番号「005」と端末 ID とを読み出し、読み出したアプリ番号「005」と端末 ID とログアウト通知とを送受信部 101 を介して、管理サーバ 600 へ送信し、処理を終了する。

(パスワード変更)

メニュー画面 161 上のボタン 166 の押下を示す操作指示情報を受け取ると、制御部 107 は、パスワードの変更を要求するパスワード変更指示を生成し、記憶部 110 からアプリ番号「005」と端末 ID 130 とを読み出し、読み出したアプリ番号「005」と端末 ID 130 と生成したパスワード変更指示とを、送受信部 601 を介して管理サーバ 600 へ送信する。

次に、送受信部 101 を介して管理サーバ 600 から、端末用パスワード変更画面データを受信する。受信した端末用パスワード変更画面データからパスワード変更画面 191 を生成し、生成したパスワード変更画面 191 を画像表示部 113 に出力し表示を指示する。図 7 は、こ

こで表示されるパスワード変更画面 191 の一例である。端末用パスワード変更画面データは、パスワード変更画面 191 を生成するためのデータであり、HTML により記述される。

次に、入力部 112 を介して、利用者による入力を受け付ける。以下の説明において、利用者により空欄 192 に入力されるパスワードを現パスワード、空欄 193 及び 194 に入力されるパスワードを新パスワードと呼称する。

取ると、受け付けた現パスワード及び新パスワードと端末共通鍵とを暗号処理部１０８へ出力し、暗号化を指示する。次に、暗号処理部１０８から暗号化現パスワードと暗号化新パスワードとを受け取る。記憶部１１０から、アプリ番号「００５」と端末ＩＤ１３０とを読み出し、読み出したアプリ番号「００５」と端末ＩＤ１３０と受け取った暗号化現パスワードと暗号化新パスワードとを送受信部１０１を介して、管理サーバ６００へ送信する。

次に、管理サーバ６００から、端末用変更完了画面データ、端末用変更失敗画面データ又は端末強制終了画面データを受信する。端末用変更完了画面データ、端末用変更失敗画面データは、それぞれ変更完了画面３０１及び変更失敗画面３１１を生成するためのデータであり、一例として、HTMLにより記述される。

端末用強制終了画面データを受信すると、受信した端末用強制終了画面データから強制終了画面３２１を生成し、生成した強制終了画面３２１を画像表示部１１３を介してモニタに表示し、処理を終了する。

端末用変更完了画面データを受信すると、受信した端末用変更完了画面データから変更完了画面３０１を生成し、生成した変更完了画面３０１を画像表示部１１３を介してモニタに表示する。図７は、ここで表示される変更完了画面３０１の一例を示している。

次に、入力部１１２を介して、利用者のボタン操作を受け付ける。入力部１１２から、変更完了画面３０１上のメニューボタン３０２の押下を示す操作指示情報を受け取ると、画像表示部１１３にメニュー画面１６１の表示を指示し、利用者によるメニューの選択へもどる。

ログアウトボタン３０３の押下を示す操作指示情報を受け取ると、制御部１０７は、ログアウト通知を生成し、記憶部１１０からアプリ番号「００５」と端末ＩＤ１３０とを読み出し、読み出したアプリ番号「００５」と端末ＩＤ１３０とログアウト通知とを送受信部１０１を介して、管理サーバ６００へ送信し、処理を終了する。

端末用変更失敗画面データを受信すると、制御部１０７は、受信した

端末用変更失敗画面データから変更失敗画面 3 1 1 を生成し、生成した変更失敗画面 3 1 1 を画像表示部 1 1 3 を介してモニタに表示する。図 8 は、ここで表示される変更失敗画面 3 1 1 の一例を示している。次に、入力部 1 1 2 を介して、利用者のボタン操作を受け付ける。入力部 1 1 2 から、変更失敗画面 3 1 1 上のメニューボタン 3 1 2 の押下を示す操作指示情報を受け取ると、画像表示部 1 1 3 にメニュー画面 1 6 1 の表示を指示し、メニューの選択の受け付けに戻る。

ログアウトボタン 3 1 3 の押下を示す操作指示情報を受け取ると、制御部 1 0 7 は、ログアウト通知を生成し、記憶部 1 1 0 からアプリ番号「0 0 5」と端末 I D 1 3 0 とを読み出し、読み出したアプリ番号「0 0 5」と端末 I D 1 3 0 とログアウト通知とを送受信部 1 0 1 を介して、管理サーバ 6 0 0 へ送信し、処理を終了する。

(5) 認証部 1 0 3

認証部 1 0 3 は、制御部 1 0 7 と外部機器との通信に先だって、秘密鍵 1 3 5 と公開鍵証明書 1 3 6 とを用いて外部機器との間で相互認証を行い、相互認証が成功した場合のみ制御部 1 0 7 と外部機器との通信を許可し、外部装置と同一の端末共通鍵を生成する。ここで、外部機器とは、具体的には、管理サーバ 6 0 0 である。

(6) 暗号処理部 1 0 8

暗号処理部 1 0 8 は、制御部 1 0 7 から各種情報と端末共通鍵とを受け取り暗号化を指示される。暗号化の指示を受け取ると、受け取った端末共通鍵を用いて受け取った各種情報に暗号化アルゴリズム E 1 を施して暗号化情報を生成し、生成した暗号化情報を制御部 1 0 7 へ出力する。

暗号処理部 1 0 8 が、制御部 1 0 7 から受け取る各種情報は、具体的には、パスワード、入力情報、現パスワード及び新パスワードである。

また、制御部 1 0 7 から各種の暗号化情報と端末共通鍵を受け取り、復号を指示される。復号の指示を受け取ると、暗号処理部は、受け取った暗号化情報に、端末共通鍵を用いて、復号アルゴリズム D 2 を施し、各種の情報を生成する。

ここで、復号アルゴリズムD2は、暗号化アルゴリズムE2により生成された暗号文を復号するアルゴリズムであり、暗号化アルゴリズムE1及びE2は一例としてDES暗号方式などの共通鍵暗号方式を用いる。DES暗号方式については、公知であるので説明を省略する。

5 (7) 画像表示部113

画像表示部113は、外部のモニタと接続されている。

画像表示部113は、制御部107から各種の画面を受け取り、画面の表示を指示される。受け取った画面から画像信号を生成し、垂直同期信号、水平同期信号を生成し、生成した垂直同期信号及び水平同期信号
10 に合わせて、画像信号をモニターへ出力する。

1. 3 アプリサーバ200

第1アプリサーバ200a～第4アプリサーバ200dは、ユーザ端末100に対して、各種のサービスを提供する。本実施の形態では、第1アプリサーバ200aは、出張費精算、第2アプリサーバ200bは
15 休暇申請、第3アプリサーバ200cは、会議室予約、第4アプリサーバ200dは、従業員購入のサービスを提供する。

アプリサーバ200は、図9の示すように、送受信部201、認証部203、制御部207、暗号処理部208、情報記憶部210、入力部212及び表示部213から構成される。

20 アプリサーバ200は、具体的には図示されていないマイクロプロセッサ及びRAM、ROMなどから構成される。前記RAM、ROMにはコンピュータプログラムが記憶されており、前記マイクロプロセッサがこれらのコンピュータプログラムの示す手順に従って動作することにより、アプリサーバ200は、その機能を達成する。

25 (1) 情報記憶部210

情報記憶部210は、ハードディスクユニットから構成され、一例として図10に示すように、パスワードテーブル221、アプリログインテーブル231、秘密鍵242、公開鍵証明書243、CRL244及び認証局公開鍵245を記憶している。また、具体的に図示していない

が、アプリサーバ２００が提供するサービスを実行するための各種プログラム及び画像データを記憶している。

パスワードテーブル２２１は、図１１に示すように、複数のパスワード情報２２３、２２４、２２５・・・から構成され、各パスワード情報は、ユーザＩＤ、氏名及びパスワードを含む。ユーザＩＤは、アプリサーバ２００の正当な利用者と１対１に対応しており、氏名は、ユーザＩＤと対応する利用者の氏名である。パスワードは、ユーザＩＤと対応する利用者がアプリサーバ２００の正当な利用者であるか否かを判断するための文字列又は数字列である。

アプリログインテーブル２３１は、図１２に示すように、複数のログイン情報２３２、２３３・・・から構成される。各ログイン情報は、ユーザＩＤ、氏名パスワード及び端末ＩＤを含む。

ユーザＩＤは、現在、アプリサーバ２００によるパスワード認証を終え、アプリサーバ２００の提供するサービスを利用中の利用者に対応しており、氏名及びパスワードは、ユーザＩＤと対応する利用者の氏名及びパスワードである。端末ＩＤは、利用者が現在使用しているユーザ端末に固有の識別情報である。

公開鍵証明書２４３は、秘密鍵２４２と対になる公開鍵の正当性を証明するものであり、証明書ＩＤ、前記公開鍵及び認証局による署名データを含む。

ＣＲＬ２４４及び認証局公開鍵２４５は、ユーザ端末１００の記憶しているＣＲＬ１３７及び認証局公開鍵１３８と同一のものであるので説明を省略する。

（２）送受信部２０１

送受信部２０１は、アプリサーバ２００のＩＰアドレス及び管理サーバ６００のＩＰアドレスを記憶している。

送受信部２０１は、制御部２０７及び認証部２０３と管理サーバ６００との間で情報の送受信を行う。

送受信部２０１が、制御部２０７と管理サーバ６００との間で送受信

する各種の情報は、図４に示すパケット１４０の形体をしている。制御部２０７から、アプリ番号、端末ＩＤ及び各種の情報からなるデータ部１４３を受け取り送信を指示される。

5 制御部２０７から送信を指示されると、受け取ったデータ部１４３に送信元としてアプリサーバ２００のＩＰアドレスを設定し、送信先としてアプリサーバ２００のＩＰアドレスを設定して送信する。

また、送受信部２０１は、管理サーバ６００以外の外部装置からの情報の受信を拒否する。具体的には、受信したパケットに含まれる送信元アドレスが管理サーバ６００のＩＰアドレスであるか否かを確認し、管理サーバ６００のＩＰアドレスでなければ受信したパケットを削除する。

(３) 入力部２１２及び表示部２１３

入力部２１２は、操作者による情報及び指示の入力を受け付け、受け付けた情報及び受け付けた指示に応じた操作指示情報を制御部２０７へ出力する。

15 表示部２１３は、制御部２０７の制御により、各種情報を表示する。

(４) 制御部２０７

制御部２０７は、上記のプロセッサがコンピュータプログラムに従って動作することにより、アプリサーバ２００００で実行する各種の情報処理を制御する。

20 制御部２０７は、管理サーバ６００から公開鍵証明書を受信し、受信した公開鍵証明書を認証部２０３へ出力し、管理サーバ６００との相互認証を指示する。認証部２０３による相互認証が成功し、認証部２０３からサーバ共通鍵を受け取ると、受け取ったサーバ共通鍵を記憶する。記憶したサーバ共通鍵を用いて、秘密通信を行い、以下に説明する各処理
25 において、安全に情報の送受信を行う。

また、制御部２０７は、アプリサーバ２００自身が提供するサービスを示すアプリ番号を記憶しており、以下の処理において、送受信部２０１を介して情報の送信を行う際、記憶しているアプリ番号と処理対象となっている利用者が使用しているユーザ端末１００の端末ＩＤと送信す

る情報とからなるデータ部 1 4 3 を生成し、生成したデータ部 1 4 3 を送受信部 2 0 1 へ出力する。以下の説明において、データ部 1 4 3 の生成については説明を省略し、単に、アプリ番号と端末 I D と各種情報と表現する。

- 5 制御部 2 0 7 は、管理サーバ 6 0 0 から、アプリサーバ 2 0 0 のアプリ番号と端末 I D とユーザ I D と暗号化パスワードとサービス開始要求とを受信する。また、管理サーバ 6 0 0 からアプリ番号と端末 I D とログアウト通知とを受信する。

- 10 制御部 2 0 7 は、管理サーバ 6 0 0 からアプリサーバ 2 0 0 と対応するアプリ番号と端末 I D とユーザ I D と暗号化現パスワードと暗号化新パスワードとパスワード変更の指示を受信する。また、管理サーバ 6 0 0 から、アプリサーバ 2 0 0 と対応するアプリ番号とユーザ I D と暗号化現パスワードと暗号化新パスワードとパスワード復旧の指示を受け取る。

- 15 以下に、制御部 2 0 7 の行うサービス提供の処理、パスワード変更の処理、パスワード復旧の処理及びログアウト処理について説明する。

(i) サービス提供の処理

- 20 サービスの提供の処理において、制御部 2 0 7 は、管理サーバ 6 0 0 から各種情報を受信するたびに、各種情報と共に受信するユーザ端末 1 0 0 の端末 I D を含むログイン情報 2 3 2 が、アプリログインテーブル 2 3 1 内に存在することを確認し、ユーザ端末 1 0 0 の利用者がログイン済みであることを確認する。以下のサービス提供の説明において、受信時のログイン済みの確認については、説明を省略する。

- 25 制御部 2 0 7 は、管理サーバ 6 0 0 からアプリ番号と処理対象となっている利用者の使用しているユーザ端末 1 0 0 の端末 I D とユーザ I D と暗号化パスワードとサービス開始要求とを受信すると、サービス提供の処理を開始する。ここでは、一例として、第 1 アプリサーバ 2 0 0 a の提供する出張費精算のサービスについて説明する。

制御部 2 0 7 は、受信した暗号化パスワードと、相互認証により生成

されたサーバ共通鍵とを暗号処理部 108 へ出力し、復号を指示する。

暗号処理部 208 からパスワードを受け取ると、パスワードテーブル 221 に受信したユーザ ID とパスワードとを含むパスワード情報が存在

- するか否かを判断する。受け取ったユーザ ID とパスワードとを含むパスワード情報がパスワードテーブル 221 内に存在しないと判断すると、
5 制御部 207 は、管理サーバ 600 の記憶しているパスワードと第 1 アプリサーバ 200a が記憶しているパスワードが一致していないことを示すパスワードエラー信号と受信したユーザ ID とを、管理サーバ 600 へ送信し、サービス提供の処理を終了する。

- 10 受信したユーザ ID とパスワードを含むパスワード情報 223 が存在すると判断すると、受信したユーザ ID と暗号処理部 208 から受け取ったパスワードを含むパスワード情報 223 を選択する。次に、受信した端末 ID と抽出した端末 ID と選択したパスワード情報 223 とからログイン情報 232 を生成し、生成したログイン情報 232 をアプリログインテーブル 231 に追加して書き込む。
15

- 次に、制御部 207 は、情報記憶部 210 から精算画面データを読み出し、ログイン情報 232 からユーザ ID と氏名を抽出し、読み出した精算画面データと抽出したユーザ ID と氏名とを基に、端末用精算画面データを生成する。次に、ログイン情報 232 から端末 ID を抽出し、
20 制御部 207 自身の記憶しているアプリ番号「001」と抽出した端末 ID と生成した端末用精算画面データとを、送受信部 201 を介して管理サーバ 600 へ送信する。

- 次に、管理サーバ 600 から、アプリ番号「001」と端末 ID と暗号化入力データを受信する。受信した暗号化入力データとサーバ共通鍵とを暗号処理部 208 へ出力し、復号を指示する。暗号処理部 108 から、入力データを受け取り、受け取った入力データを基に、利用者の出張費の精算処理を行う。
25

出張費の精算処理が終了すると、情報記憶部 210 から精算終了画面データを読み出し、読み出した精算終了画面データとログイン情報 23

2 から、端末用精算終了画面データを生成し、アプリ番号「001」とログイン情報232に含まれる端末IDと生成した端末用精算終了画面データとを管理サーバ600へ送信し、出張費精算のサービスを終了する。

5 (ii) パスワード変更

制御部207は、管理サーバ600から、アプリサーバ200と対応するアプリ番号とパスワード変更の対象となっている利用者が使用しているユーザ端末100の端末IDとユーザIDと暗号化現パスワードと暗号化新パスワードとパスワード変更の指示を受信すると、受信した端末IDを一時的に記憶する。

次に、受信した暗号化現パスワードと暗号化新パスワードとサーバ共通鍵とを暗号処理部208へ出力し、復号を指示する。暗号処理部208から、現パスワードと新パスワードとを受け取り、受け取った現パスワードと受信したユーザIDとを含むパスワード情報223をパスワードテーブル221から選択する。次に選択したパスワード情報223のパスワードを、新パスワードに書き換える。

書き換えが正常に終了すると、制御部207は、終了信号「1」を生成する。ハードディスク不良などにより、書き換えが失敗すると、終了信号「0」を生成し、アプリサーバ200自身のアプリ番号と一時的に記憶している端末IDと生成した終了信号とを送受信部201を介して、管理サーバ600へ送信し、パスワード変更の処理を終了する。

(iii) パスワード復旧処理

管理サーバ600から、アプリサーバ200と対応するアプリ番号と端末IDとユーザIDと暗号化現パスワードと暗号化新パスワードとパスワード復旧の指示を受け取ると、端末IDを一時的に記憶する。次に、制御部207は、受け取った暗号化現パスワードと暗号化新パスワードとサーバ共通鍵とを暗号処理部208へ出力し、復号を指示する。

暗号処理部208から、現パスワードと新パスワードとを受け取り、受け取った新パスワードと受信したユーザIDとを含むパスワード情報

2 2 3 をパスワードテーブル 2 2 1 から選択する。選択したパスワード情報 2 2 3 に含まれるパスワードを受け取った現パスワードに書き換える。

- 5 パスワードの書き換えが正常に終了すると、終了信号「1」を生成する。パスワードの書き換えが失敗すると、終了信号「0」を生成する。次に、アプリサーバ 2 0 0 自身と対応するアプリ番号と一時的に記憶した端末 I D と生成した終了信号とを送受信部 2 0 1 を介して、管理サーバ 6 0 0 へ送信し、処理を終了する。

(iv) ログアウト処理

- 10 制御部 2 0 7 は、送受信部 2 0 1 を介して、管理サーバ 6 0 0 から、アプリ番号とユーザ端末 1 0 0 の端末 I D とログアウト通知を受信すると、アプリログインテーブル 2 3 1 内で受信した端末 I D を含むログイン情報 2 3 2 を探す。受信した端末 I D を含むログイン情報がアプリログインテーブル 2 3 1 内に存在しなければ、そのままログアウト処理を終了する。

15 受信した端末 I D を含むログイン情報 2 3 2 がアプリログインテーブル 2 3 1 内に存在すれば、受信した端末 I D を含むログイン情報 2 3 2 を削除し、ログアウト処理を終了する。

(5) 認証部 2 0 3

- 20 認証部 2 0 3 は、制御部 2 0 7 と外部機器との通信に先だって、秘密鍵 2 4 2 と公開鍵証明書 2 4 3 とを用いて外部機器との間で相互認証を行い、相互認証が成功した場合のみ制御部 2 0 7 と外部機器との通信を許可し、外部装置と同一のサーバ共通鍵を生成する。ここで、外部機器とは、具体的には、管理サーバ 6 0 0 である。

- 25 (6) 暗号処理部 2 0 8

暗号処理部 2 0 8 は、制御部 2 0 7 から各種の情報とサーバ共通鍵を受け取り暗号化を指示される。暗号化の指示を受け取ると、受け取ったサーバ共通鍵を用いて受け取った情報に暗号化アルゴリズム E 4 を施し、暗号化情報を生成し、生成した暗号化情報を、制御部 2 0 7 へ出力する。

また、制御部 207 から各種の暗号化情報とサーバ共通鍵とを受け取り復号を指示される。復号の指示を受け取ると、受け取ったサーバ共通鍵を用いて、受け取った暗号化情報に復号アルゴリズム D3 を施して、情報を生成し、生成した情報を制御部 207 へ出力する。

- 5 暗号処理部 208 が、制御部 207 から受け取る、暗号化情報は、具体的には、暗号化パスワード、暗号化入力データ、暗号化現パスワード及び暗号化新パスワードである。

ここで、復号アルゴリズム D3 は、暗号化アルゴリズム E3 により生成された暗号文を復号するアルゴリズムであり、暗号化アルゴリズム E3 及び E4 は、一例として DES 暗号方式などの共通鍵暗号方式である。

1. 4 管理サーバ 600

管理サーバ 600 は、図 13 に示すように、送受信部 601、認証部 603、パスワード変更部 606、制御部 607、暗号処理部 608、パスワード復旧部 614、変更判定部 609、変更結果通知部 615、
15 情報記憶部 610、入力部 612 及び表示部 613 から構成される。

管理サーバ 600 は、具体的には図示されていないマイクロプロセッサ、RAM、ROM 及びハードディスクから構成される。前記 RAM、ROM 及びハードディスクにはコンピュータプログラムが記憶されており、前記マイクロプロセッサが前記コンピュータプログラムに従って動作することにより、管理サーバ 600 は、その機能を達成する。

（1）情報記憶部 610

情報記憶部 610 は、ハードディスクユニットから構成され、一例として、図 14 に示すように、パスワードテーブル 621、ログインテーブル 631 ルーティングテーブル 641、パスワード変更テーブル 651、秘密鍵 661、公開鍵証明書 662、CRL 663 及び認証局公開鍵 664 を記憶している。

パスワードテーブル 621 は、アプリサーバ 200 の記憶しているパスワードテーブル 221 と同様の構成であるので、説明を省略する。

ログインテーブル 631 は、図 15 に示すように、複数のログイン情

報 6 3 2、6 3 3、6 3 4・・・から構成され、各ログイン情報は、ユーザ I D、氏名、パスワード、端末 I D 及び処理状況を含む。

ユーザ I D は、管理サーバ 6 0 0 によるパスワードの認証を終え、現在各種サービスを利用中の利用者に対応しており、氏名及びパスワードは、ユーザ I D の示す利用者の氏名及びパスワードである。端末 I D は、ユーザ I D の示す利用者が現在使用しているユーザ端末に固有の識別情報である。処理状況は、端末 I D の示すユーザ端末と管理サーバ 6 0 0 及びアプリサーバ 2 0 0 間で行っている処理の種類を示しており、パスワードの変更処理を行っているときは「パスワード変更中」、アプリサーバ 2 0 0 による各種サービスに係る処理を行っているときは「通常」に設定されている。

ルーティングテーブル 6 4 1 は、図 1 6 に示すように、複数のルート情報 6 4 2、6 4 3・・・から構成され、各ルート情報は、アプリ番号、ホスト名、I P アドレス及びポート番号を含む。

アプリ番号は、第 1 アプリサーバ 2 0 0 a ～第 4 アプリサーバ 2 0 0 d と対応しており、各アプリサーバが提供するサービスを示す識別情報である。これは、ユーザ端末 1 0 0 が記憶しているアプリ番号表 1 2 0 に含まれるアプリ番号と同一のものである。ホスト名は、アプリ番号と対応するアプリサーバ 2 0 0 を特定する識別情報である。I P アドレスは、前記アプリサーバのネットワーク上の位置を示す I P アドレスであり、ポート番号は、管理サーバ 6 0 0 が、アプリサーバ 2 0 0 へ情報を送信する際に指定する送信先ポート番号である。

パスワード変更テーブル 6 5 1 は、図 1 7 に示すように、複数の変更情報 6 5 2、6 5 3、6 5 4・・・から構成される。各変更情報は、ユーザ I D、現行パスワード及び新パスワードを含む。

ユーザ I D は、アプリサーバ 2 0 0 及び管理サーバ 6 0 0 の正当な利用者に割り当てられた識別情報である。現パスワードは、パスワード変更処理を行う時点で利用者が使用しているパスワードであり、新パスワードは、パスワード変更処理において、利用者が設定した新しいパスワード

ードである。具体的には、現パスワードは、図7の示すパスワード変更画面191内の空欄192に入力される文字列であり、新パスワードは、空欄193及び194に入力される文字列である。

5 公開鍵証明書662は、秘密鍵661と対になる公開鍵の正当性を証明するものであり、証明書ID、前記公開鍵及び認証局による署名データを含む。

CRL663及び認証局公開鍵664は、ユーザ端末100の記憶しているCRL137及び認証局公開鍵138と同一であるので説明を省略する。

10 また、情報記憶部610は、具体的には図示していないが、各種の画面データを記憶している。

(2) 送受信部601

送受信部601は、ユーザ端末100の端末IDとユーザ端末100のIPアドレスとを対応付けて記憶する。また、管理サーバ600のIP
15 IPアドレスを記憶している。

送受信部601は、管理サーバ600内の各部と外部機器との間で情報の送受信を行う。

送受信部601が、送受信する各種情報は、一例として図4に示すパケット140の形体である。

20 送受信部601は、制御部607、パスワード変更部606又はパスワード復旧部614から、アプリ番号とユーザ端末100の端末IDと各種の情報からなるデータ部143を受け取り、送信を指示される。

制御部607から、ユーザ端末100への送信を指示されると、送信元を管理サーバ600のIPアドレスに設定し、端末IDを基に送信先
25 をユーザ端末100のIPアドレスに設定し、受け取ったデータ部143を送信する。また、制御部607又はパスワード変更部606から情報を受け取り、アプリサーバ200への送信を指示されると、アプリ番号を基にルーティングテーブル641からルート情報を選択し、選択したルート情報からIPアドレスとポート番号を抽出し、送信先アドレス

を抽出したIPアドレスに設定し、送信元を管理サーバ600のIPアドレスに設定し、送信先ポート番号を抽出したポート番号に設定して送信する。

(3) 入力部612及び表示部613

- 5 入力部612は、操作者による情報及び指示の入力を受け付け、受け付けた情報及び受け付けた指示に応じた操作指示情報を制御部607へ出力する。

表示部613は、制御部607からの指示により、各種情報を表示する。

10 (4) パスワード変更部606

- パスワード変更部606は、制御部607から、アプリ番号と端末IDとユーザIDと暗号化現パスワードと暗号化新パスワードとを受け取りパスワード変更を指示される。制御部607からパスワード変更を指示されると以下に説明するパスワード変更処理を行う。なお、以下の説明において、データ部143の生成については説明を省略し、単にアプリ番号、端末ID及び各種情報の出力と表現する。
- 15

(パスワード変更処理)

- パスワード変更部606は、制御部607から、アプリ番号と端末IDと暗号化現パスワードと暗号化新パスワードとを受け取りパスワード変更を指示されると、アプリサーバ200に対してパスワードの変更を指示するパスワード変更指示を生成し、受け取ったユーザIDとアプリ番号とユーザIDと暗号化現パスワードと暗号化新パスワードと生成したパスワード変更指示とを送受信部601に出力し、アプリサーバ200へ送信を指示する。
- 20

- 送信と同時に、パスワード変更部606は、アプリサーバ200へパスワード変更指示を送信したことを示す変更指示送信済信号を生成し、生成した変更指示送信済信号と制御部607から受け取ったアプリ番号と端末IDとを変更判定部609へ出力する。
- 25

(5) パスワード復旧部614

パスワード復旧部 614 は、制御部 607 からアプリ番号と端末 ID とユーザ ID と暗号化現パスワードと暗号化新パスワードとを受け取りパスワード復旧を指示される。

5 また、変更判定部 609 からパスワード復旧指示の再送信を指示される。

制御部 607 からパスワード復旧を指示されると以下に説明するパスワード復旧処理を開始する。なお、以下の説明において、データ部 143 の生成については説明を省略し、単にアプリ番号、端末 ID 及び各種情報の出力と表現する。

10 (パスワード復旧処理)

パスワード復旧部 614 は、制御部 607 から、アプリ番号と端末 ID とユーザ ID と暗号化現パスワードと暗号化新パスワードとを受け取りパスワード復旧を指示されると、アプリサーバ 200 に対してパスワードを現パスワードに戻すことを指示するパスワード復旧指示を生成し、
15 受け取ったアプリ番号と端末 ID と暗号化現パスワードと暗号化新パスワードと生成したパスワード復旧指示とを一時的に記憶する。次に、受け取ったアプリ番号と端末 ID と暗号化現パスワードと暗号化新パスワードと生成したパスワード復旧指示とを送受信部 601 へ出力し、アプリ番号と対応するアプリサーバ 200 への送信を指示する。

20 送信と同時に、パスワード復旧部 614 は、アプリサーバ 200 へパスワード復旧指示を送信したことを示す復旧送信済信号を生成し、生成した復旧送信済信号と記憶しているアプリ番号と端末 ID とを変更判定部 609 へ出力する。

変更判定部 609 から、パスワード復旧指示の再送信を指示されると、
25 パスワード復旧部 614 は、記憶しているアプリ番号と端末 ID と暗号化現パスワードと暗号化新パスワードとパスワード復旧指示とを読み出し、読み出したアプリ番号と端末 ID と暗号化現パスワードと暗号化新パスワードとパスワード復旧指示とを送受信部 601 を介して再送信する。

再送信と同時に、復旧送信済信号を変更判定部 609 へ出力する。

(6) 変更判定部 609

変更判定部 609 は、時間の経過に伴って経過時間を計測する time カウンタとパスワード復旧指示の送信回数を数える回数カウンタとを
5 備える。

また、変更判定部 609 は、あらかじめ、最大待ち時間と制限回数を記憶している。最大待ち時間は、パスワード変更部 606 又はパスワード復旧部 614 がパスワード変更指示又はパスワード復旧指示を送信してから終了信号を受け取るまでの待機時間の上限値「1 秒」である。パスワード変更指示を送信してから最大待ち時間を超えて終了信号を受信しなければ、パスワードの変更失敗を示す変更終了信号「0」を生成する。パスワード復旧指示を送信してから、最大待ち時間を超えて終了信号を受信しなければ、パスワード復旧部 614 にパスワード復旧指示の再送信を指示する。

15 制限回数は、1 台のアプリサーバ 200 へパスワード復旧指示を送信できる回数の最大値「3 回」である。パスワード復旧指示の送信回数が「3 回」を超えると、パスワード復旧の失敗を示す復旧終了信号「0」を生成する。

20 変更判定部 609 は、パスワード変更部 606 から変更指示送信済信号とアプリ番号と端末 ID とを受け取る。

変更判定部 609 は、パスワード復旧部 614 から、復旧指示送信済信号とアプリ番号と端末 ID とを受け取る。また、パスワード復旧部 614 から復旧指示送信済信号のみを受け取る。

25 以下に変更判定部 609 の行う (i) パスワード変更の判定処理と (ii) パスワード復旧の判定処理について説明する。

(i) パスワード変更の判定処理

変更判定部 609 は、パスワード変更部 606 から変更指示送信済信号とアプリ番号と端末 ID とを受け取ると、受け取ったアプリ番号と端末 ID とを内部に一時的に記憶する。

また、変更指示送信済信号を受け取ると同時に、timeカウンタを0に初期化し、経過時間の計測を開始する。

次に、送受信部601を介してアプリサーバ200から終了信号を受信すると、受信した終了信号を判別し、終了信号が「1」であれば、アプリサーバ200のパスワード変更が成功であることを示す変更終了信号「1」を生成する。受信した終了信号が「0」であると判断すると、アプリサーバ200のパスワード変更が失敗であることを示す変更終了信号「0」を生成する。

また、アプリサーバ200から終了信号を受信していない場合、timeカウンタの値と最大待ち時間とを比較する。timeカウンタが最大待ち時間を超えていないと判断すると、終了信号を受信するかtimeカウンタが最大待ち時間を超えるまで、timeカウンタと最大待ち時間の比較を繰り返す。

timeカウンタの値が最大時間を超えていると判断すると、変更判定部609は、アプリサーバ200のパスワード変更が失敗であると判断し、変更終了信号「0」を生成する。

次に、記憶しているアプリ番号と端末IDと生成した変更終了信号とを、制御部607へ出力する。

(ii) パスワード復旧の判定処理

変更判定部609は、パスワード復旧部614から、復旧指示送信済信号とアプリ番号と端末IDとを受け取ると、受け取ったアプリ番号と端末IDとを内部に一時的に記憶し、回数カウンタを0に初期化する。

また、復旧指示送信済信号を受け取ると同時に、パスワード変更部606は、timeカウンタを0に初期化して経過時間の計測を開始する。

パスワード復旧部614から、復旧指示送信済信号のみを受け取ると、回数カウンタの初期化は行わず、timeカウンタを0に初期化して経過時間の計測を開始する。

次に、送受信部601を介して、アプリサーバ200からの終了信号を受信すると、受信した終了信号を判別し、終了信号が「1」であれば、

アプリサーバ200のパスワード復旧が成功であることを示す復旧終了信号「1」を生成する。

受信した終了信号が「0」であると判断すると、回数カウンタに1加算する。次に回数カウンタの値と制限回数とを比較する。回数カウンタが制限回数を超えていないと判断すると、パスワード復旧部614にパスワード復旧指示の再送信を指示する。

また、アプリサーバ200からの終了信号を受信していない場合、timeカウンタと最大待ち時間とを比較する。timeカウンタが最大待ち時間を超えていないと判断すると、終了信号を受信するか経過時間が最大待ち時間を超えるまで、timeカウンタと最大待ち時間の比較を繰り返す。

timeカウンタが、最大待ち時間を超えていると判断すると、回数カウンタに1加算する。次に、回数カウンタと制限回数を比較する。回数カウンタが、制限回数以内であれば、パスワード復旧部614にパスワード復旧指示の再送信を指示する。

回数カウンタが、制限回数を超えていると判断すると、パスワード復旧が失敗であることを示す復旧終了信号「0」を生成する。

復旧終了信号を生成すると、次に、記憶しているアプリ番号と端末IDと生成した復旧終了信号とを制御部607へ出力する。

(7) 制御部607

制御部607は、上記のプロセッサがコンピュータプログラムに従って動作することにより、管理サーバ600で実行する各種の情報処理を制御する。

制御部607は、アプリサーバ200とアプリサーバ200が提供するサービスを示すアプリ番号とを対応付けて記憶している。

制御部607は、送受信部601を介してユーザ端末100から公開鍵証明書を受信する。

ユーザ端末100から公開鍵証明書を受信すると、受信した公開鍵証明書を認証部603へ出力し、相互認証を指示する。認証部603によ

る相互認証が終了し、端末共通鍵を受け取る。受け取った端末共通鍵を用いて秘密通信をすることにより、ユーザ端末１００との間で以下に説明する処理を安全に行う。

また、制御部６０７が、送受信部６０１を介して送受信する情報は、
5 図４に示すようなパケット１４０の形体である。制御部６０７は、受信したアプリ番号を判別し、利用者が利用しようとするサービスを提供する機器がアプリサーバ２００又は管理サーバ６００のいずれであるかを判断する。制御部６０７は、各種情報を送信する際、送信する情報と処理の対象となっている利用者の使用しているユーザ端末１００の端末ID
10 IDと処理を実行する機器と対応するアプリ番号からなるデータ部１４３を生成し、生成したデータ部１４３を送受信部６０１へ出力し、送信を指示する。ここで、処理を実行する機器とは、アプリサーバ２００及び管理サーバ６００である。

以下に説明する制御部６０７の行う処理において、上記のようなデータ部１４３の生成に関する説明は省略し、単にアプリ番号と端末IDと各種情報と表現する。
15

制御部６０７は、利用者のログイン処理、各種サービスの中継処理、パスワード変更制御、パスワード復旧制御及びログアウト処理を行う。以下に、利用者のログイン処理、各種サービスの中継処理、パスワード
20 変更制御、パスワード復旧制御及びログアウト処理について説明する。

(i) 利用者のログイン処理

制御部６０７は、認証部６０３による、相互認証が終了すると、認証部６０３から端末共通鍵を受け取り、受け取った端末共通鍵を記憶する。制御部６０７は、情報記憶部６１０からログイン画面データを読み出し、
25 送受信部６０１を介して読み出したログイン画面データをユーザ端末１００へ送信する。

次に、ユーザ端末１００からアプリ番号「００５」と端末IDとユーザIDと暗号化パスワードとを受信し、受信した暗号化パスワードと端末共通鍵とを暗号処理部６０８に出力し、復号を指示する。暗号処理部

608からパスワードを受け取ると、パスワードテーブル621内で、受信したユーザIDと受け取ったパスワードを含むパスワード情報を検索する。受信したユーザIDと受け取ったパスワードを含むパスワード情報が存在しないと判断すると、再度、ログイン画面データをユーザ端末100へ送信する。

受信したユーザIDと受け取ったパスワードを含むパスワード情報が存在すると判断すると、受信したユーザIDと受け取ったパスワードを含むパスワード情報を選択する。受信した端末IDと選択したパスワード情報とを基に、ログイン情報632を生成し、生成したログイン情報632をログインテーブル631に追加して書き込む。このとき、処理状況は「通常」に設定する。これにより、ログイン処理完了と判断する。

これ以降の処理において、ユーザ端末100から各種情報を受信するたびに、各種情報と共に受信する端末IDを含むログイン情報632がログインテーブル631内に存在することを確認し、ユーザ端末100の利用者がログイン済みであることを確認する。以下の説明において、ログイン済みの確認については、詳細な説明を省略する。

次に、情報記憶部610からメニュー画面データを読み出し、読み出したメニュー画像データと書き込んだログイン情報632に含まれるユーザID及び氏名を基に、端末用メニュー画面データを生成し、生成した端末用メニュー画面データを送受信部601を介して、ユーザ端末100へ送信する。次に、送受信部601を介して、ユーザ端末100からアプリ番号と端末IDとサービス開始要求又はアプリ番号と端末IDとパスワード変更指示を受信する。アプリ番号と端末IDとサービス開始要求を受信するとユーザ端末100とアプリサーバ200との中継処理を行い、アプリ番号と端末IDとパスワード変更指示を受信するとパスワード変更処理及びパスワード復旧処理を行う。

(ii) 各種サービスの中継処理

制御部607は、アプリ番号と端末IDサービス開始要求を受信すると、以下に説明する手順で、受信したアプリ番号の示すアプリサーバ2

00とユーザ端末100との間で中継処理を行う。

ここでは、第1アプリサーバ200aとユーザ端末100との間の中継処理について説明する。

5 制御部607は、ユーザ端末100の利用者がログイン済みであることを確認し、認証部603へアプリサーバ200aとの相互認証を指示する。認証部603による相互認証が終了し、認証部603からサーバ共通鍵を受け取り、受け取ったサーバ共通鍵を記憶する。

次に、ログインテーブル631内で受信した端末ID含むログイン情報632を選択し、選択したログイン情報632からユーザIDとパスワードを抽出する。抽出したパスワードとサーバ共通鍵とを暗号処理部608へ出力し、パスワードの暗号化を指示する。次に、暗号処理部608から暗号化パスワードを受け取る。ユーザ端末100から受信したアプリ番号「001」と端末IDとサービス開始要求と読み出したユーザIDと暗号処理部608から受け取った暗号化パスワードとを、送受信部601へ出力し、第1アプリサーバ200aへの送信を指示する。

次に、制御部607は、送受信部601を介して、アプリサーバ200aからアプリ番号「001」と端末IDとパスワードエラー信号とユーザID又はアプリ番号「001」と端末IDと端末用精算画面データを受信する。

20 アプリ番号「001」と端末IDとパスワードエラー信号とユーザIDとを受信すると、制御部607は、情報記憶部610から強制終了画面データ読み出す。次に受信したユーザIDを含むログイン情報632からユーザIDと氏名を抽出する。

読み出した強制終了画面データと抽出したユーザIDと氏名とを基に、
25 端末用強制終了画面データを生成し、送受信部601を介して、受信した端末IDと生成した端末用強制終了画面データをユーザ端末100へ送信する。次に、受信したユーザIDとエラー画面データとから、エラー画面331を生成し、表示部613へ出力し、パスワードの不一致が発生していることを管理サーバ600の操作者に通知する。

アプリ番号「００１」と端末ＩＤと端末用精算画面データとを受信すると、送受信部６０１を介して、受信したアプリ番号「００１」と端末ＩＤと端末用精算画面データとをユーザ端末１００へ送信する。

次に、送受信部６０１を介して、ユーザ端末１００から、アプリ番号
5 「００１」、端末ＩＤ及び暗号化入力データを受信する。受信した端末ＩＤを基に、ユーザ端末１００の利用者がログイン済みであることを確認する。

次に、受信した暗号化入力データと端末共通鍵とを暗号処理部６０８へ出力し、暗号化入力データの復号を指示する。暗号処理部６０８から
10 入力データを受け取る。次に、受け取った入力データとサーバ共通鍵とを暗号処理部６０８へ出力し、入力データの暗号化を指示する。暗号処理部６０８から暗号化入力データを受け取る。

次に、制御部６０７は、アプリ番号「００１」と受信した端末ＩＤと暗号処理部６０８から受け取った暗号化入力データとを送受信部６０１
15 を介して、第１アプリサーバ２００ａへ送信する。

次に、送受信部６０１を介して、アプリサーバ２００ａから、アプリ番号「００１」、端末ＩＤ及び端末用精算終了画面データを受信する。受信したアプリ番号「００１」、端末ＩＤ及び端末用精算終了画面データをユーザ端末１００へ送信する。

20 (iii) パスワード変更制御

制御部６０７は、受付処理、パスワード変更指示、結果通知の順序でパスワード変更制御を行う。以下に、受付処理、パスワード変更指示及び結果通知の処理について説明する。

(iii-a) 受付処理

25 制御部６０７は、送受信部６０１を介して、ユーザ端末１００からアプリ番号「００５」と端末ＩＤとパスワード変更指示とを受信する。次に、ユーザ端末１００の利用者がログイン済みであることを確認する。次に、情報記憶部６１０からパスワード変更画面データを読み出し、読み出したパスワード変更画面データとログイン情報６３２とを基に、

端末用パスワード変更画面データを生成し、生成した端末用パスワード変更画面データを送受信部 601 を介して、ユーザ端末 100 へ送信する。

次に、送受信部 601 を介して、ユーザ端末 100 からアプリ番号「005」と端末 ID と暗号化現パスワードと暗号化新パスワードとを受信する。制御部 607 は、受信した端末 ID を含む、ログイン情報 632 を選択し、選択したログイン情報 632 の処理状況を「パスワード変更中」に書き換える。

次に、受信した暗号化現パスワードと暗号化新パスワードと端末共通鍵とを暗号処理部 608 へ出力し、暗号化現パスワードと暗号化新パスワードの復号を指示する。暗号処理部 608 から、生成された現パスワードと新パスワードとを受け取る。

次に、書き換えたログイン情報 632 からユーザ ID を読み出し、パスワードテーブル 621 上で、読み出したユーザ ID と受け取った現パスワードとを含むパスワード情報の有無を確認する。読み出したユーザ ID と受け取った現パスワードとを含むパスワード情報が存在しないと判断すると、送受信部 601 を介して、ユーザ端末 100 へパスワード変更画面を再度送信し、現パスワードと新パスワードの再入力を促す。

パスワードテーブル 621 上に、読み出したユーザ ID と受け取った現パスワードとを含むパスワード情報が存在すると判断すると、次に、読み出したユーザ ID を含むパスワード変更情報 652 をパスワード変更テーブル 651 から選択する。選択したパスワード変更情報 652 に含まれる現パスワードを暗号処理部 608 から受け取った現パスワードに書き換え、選択したパスワード変更情報に含まれる新パスワードを暗号処理部 608 から受け取った新パスワードに書き換える。

(iii-b) パスワード変更処理

次に、制御部 607 は、以下に説明する手順で第 1 アプリサーバ 200a ~ 第 4 アプリサーバ 200d のパスワード変更を行う。

制御部 607 は、認証部 603 へ、第 1 アプリサーバ 200a との相

互認証を指示する。認証部 603 による相互認証が終了し、認証部 603 からサーバ共通鍵を受け取り記憶する。次に、パスワード変更情報 652 から現パスワードと新パスワードとを抽出し、抽出した現パスワードと新パスワードと第 1 アプリサーバ 200a との相互認証により生成されたサーバ共通鍵とを暗号処理部 608 へ出力し、現パスワードと新パスワードの暗号化を指示する。

次に、暗号処理部 608 から暗号化現パスワードと暗号化新パスワードとを受け取る。パスワード変更情報 652 からユーザ ID を抽出する。次に、制御部 607 は、第 1 アプリサーバ 200a と対応するアプリ番号「001」とユーザ端末 100 の端末 ID と抽出したユーザ ID と受け取った暗号化現パスワードと暗号化新パスワードとをパスワード変更部 606 へ出力しパスワード変更を指示する。

次に、変更判定部 609 からアプリ番号「001」と端末 ID と変更終了信号を受け取る。受け取った変更終了信号がパスワード変更成功を示す「1」であれば第 1 アプリサーバ 200a のパスワード変更が成功であると判断する。

受け取った変更終了信号が「0」であると判断すると、第 1 アプリサーバ 200a のパスワード変更が失敗であると判断し、第 2 アプリサーバ 200b 以降のパスワード変更を中止し、パスワード復旧制御へ処理を移す。

第 1 アプリサーバ 200a のパスワード変更が成功であると判断すると、同様に、相互認証、現パスワードと新パスワードの暗号化、パスワード変更の指示及び変更終了信号の取得の手順で第 2 アプリサーバ 200b のパスワード変更を行う。

第 2 アプリサーバ 200b のパスワード変更が成功であれば、同様に第 3 アプリサーバ 200c のパスワード変更を行い、失敗であれば、第 3 アプリサーバ 200c 及び第 4 アプリサーバ 200d のパスワード変更を中止し、パスワード復旧処理へ移る。

第 3 アプリサーバ 200c のパスワード変更が成功であれば、続いて

第4アプリサーバ200dのパスワード変更を行い、失敗であれば、第4アプリサーバ200dのパスワード変更を中止し、パスワード復旧処理に移る。

- 5 第4アプリサーバ200dのパスワード変更が成功であれば、以下の結果通知を行い、失敗であれば、パスワード復旧処理を行う。

(iii-c) 結果通知

- 10 第1アプリサーバ200a～第4アプリサーバ200dのパスワード変更が全て成功すると、制御部607は、情報記憶部610の記憶しているパスワードテーブル621内において、パスワード変更部606へ出力したユーザIDを含むパスワード情報を選択し、選択したパスワード情報に含まれるパスワードを、新パスワードに書き換える。次に、ログインテーブル631から、出力したユーザIDを含むログイン情報632を選択し、選択したログイン情報632に含まれるパスワードを新パスワードに書き換える。

- 15 次に、パスワード変更の完了を示す完了信号を生成し、書き換えたログイン情報632からユーザIDと氏名とを抽出し、変更結果通知部615に生成した完了信号とユーザIDと端末IDとを出力し、ユーザ端末100への結果通知を指示する。

次に、ログイン情報632の処理状況を「通常」に書き換える。

- 20 (iv) パスワード復旧処理

上記の(iii)において説明したパスワード変更処理の途中で何れかのアプリサーバ200のパスワード変更が失敗すると、制御部607は、パスワード復旧の処理を行う。

- 25 具体的には、制御部607は、変更判定部609から変更終了信号「0」と共に受け取ったアプリ番号により、パスワード変更が失敗したアプリサーバ200を判別する。第1アプリサーバ200a～第3アプリサーバ200cのパスワード変更処理は成功し、第4アプリサーバ200dのパスワード変更処理が失敗であると判断すると、第3アプリサーバ200c～第1アプリサーバ200aの順にアプリサーバのパスワード復

旧処理を行い、次に、失敗通知処理を行う。

第1アプリサーバ200aと第2アプリサーバ200bのパスワード
変更処理は成功し、第3アプリサーバ200cのパスワード変更処理が
失敗であると判断すると、第2アプリサーバ200b～第1アプリサー
5 バ200aの順にアプリサーバのパスワード復旧処理を行い、次に、失
敗通知処理を行う。

第1アプリサーバ200aのパスワード変更処理は成功し、第2アプ
リサーバ200cのパスワード変更処理が失敗であると判断すると、第
1アプリサーバ200aにアプリサーバのパスワード復旧処理を行い、
10 次に、失敗通知処理を行う。

第1アプリサーバ200aのパスワード変更処理が失敗であると判断
すると、失敗通知処理のみを行う。

また、何れかのアプリサーバ200において、アプリサーバのパスワ
ード復旧処理が失敗すると、エラー処理を行う。

15 以下に、アプリサーバのパスワード復旧処理、失敗通知処理及びエラ
ー処理の詳細を説明する。

(iv-a) アプリサーバのパスワード復旧処理

制御部607は、パスワード変更情報652から現パスワードと新パ
スワードとを抽出し、抽出した現パスワードと新パスワードと該当する
20 アプリサーバ200のサーバ共通鍵とを暗号処理部608に出力し、現
パスワードと新パスワードとの暗号化を指示する。暗号処理部608か
ら、暗号化現パスワードと暗号化新パスワードとを受け取り、アプリサ
ーバ200に対応するアプリ番号とユーザ端末100の端末IDとパス
ワード変更情報652に含まれるユーザIDと受け取った暗号化現パス
25 ワードと暗号化新パスワードとをパスワード変更部606へ出力し、
パスワード復旧を指示する。

次に、パスワード変更部606からアプリ番号と端末IDと復旧終了
信号とを受け取る。受け取った復旧終了信号がパスワード復旧の成功を
示す「1」であれば、受け取ったアプリ番号と対応するアプリサーバ2

00のパスワード復旧が成功であると判断し、次のアプリサーバ200のパスワード復旧又は失敗通知処理を行う。

受け取った復旧終了信号がパスワード復旧失敗を示す「0」であると、該当するアプリサーバ200のパスワード復旧が失敗であると判断する。

- 5 アプリサーバ200のパスワード復旧が失敗であると判断すると、他のアプリサーバ200の復旧処理及び失敗通知の処理を行わず、後述するエラー処理を行う。

(iv-b) 失敗通知処理

- 10 制御部607は、パスワード復旧の失敗を示す失敗信号を生成し、変更判定部609から受け取った端末IDを含むログイン情報632を選択し、選択したログイン情報632からユーザIDと氏名を抽出し、生成した失敗信号と抽出したユーザIDと氏名とを変更結果通知部615へ出力し、結果通知を指示する。

- 15 次に、ログイン情報632の処理状況を「通常」に書き換え処理を終了する。

(iv-c) エラー処理

- 20 アプリサーバ200何れかのパスワード復旧の処理が失敗であると判断すると、制御部607は、情報記憶部610から強制終了画面データを読み出し、読み出した強制終了画面データとログイン情報632に含まれるユーザIDと氏名を基に端末用強制終了画面データを生成し、生成した端末用強制終了画面データを、送受信部601を介して、ユーザ端末100へ送信する。

- 25 次に、情報記憶部610からエラー画面データを読み出し、読み出したエラー画面データとログイン情報632に含まれるユーザIDからエラー画面331を生成し、生成したエラー画面331を表示部613に表示し、操作者にエラー発生を通知する。図18は、ここで表示されるエラー画面331の一例である。

(v) ログアウト処理

制御部607は、ユーザ端末100から、送受信部601を介して、

アプリ番号「００５」と端末ＩＤとログアウト通知とを受信する。ログ
アウト通知を受信すると、受信した端末ＩＤとログアウト通知とを、送
受信部６０１を介して第１アプリサーバ２００ａ～第４アプリサーバ２
００ｄへ送信する。次に、受信した端末ＩＤを含むログイン情報６３２
５ をログインテーブル６３１から削除する。

（８）変更結果通知部６１５

変更結果通知部６１５は、制御部６０７から完了信号とユーザＩＤと
端末ＩＤと結果通知の指示を受け取る。

また、制御部６０７から失敗信号とユーザＩＤと氏名と結果通知の指
示を受け取る。
１０

完了信号とユーザＩＤと端末ＩＤと結果通知の指示を受け取ると、変
更結果通知部６１５は、情報記憶部６１０から変更完了画面データを読
み出し、読み出した変更完了画面データと受け取ったユーザＩＤと氏名
とを基に、端末用変更完了画面データを生成し、生成した端末用変更完
了画面データをユーザ端末１００へ送信する。
１５

失敗信号とユーザＩＤと端末ＩＤと結果通知の指示を受け取ると、変
更結果通知部６１５は、情報記憶部６１０から変更失敗画面データを読
み出し、読み出した更失敗画面データと、受け取ったユーザＩＤと氏名
を基に、端末用変更失敗画面データを生成し、生成した端末用変更失敗
画面データを送受信部６０１を介して、ユーザ端末１００へ送信する。
２０

（９）認証部６０３

認証部６０３は、制御部６０７の指示によりインターネット２０と接
続されている外部機器と相互認証を行い共通鍵を生成する。

ここで、外部装置とはユーザ端末１００及びアプリサーバ２００であ
り、ユーザ端末１００との間では、端末共通鍵を共有し、各アプリサー
バ２００との間では、それぞれのアプリサーバとサーバ共通鍵を共有す
る。
２５

、（１０）暗号処理部６０８

暗号処理部６０８は、制御部６０７からの指示により各種情報の暗号

化及び復号を行う。

- 5 具体的には、制御部 607 から、暗号化パスワードと端末共通鍵、暗号化入力データと端末共通鍵又は暗号化現パスワードと暗号化新パスワードと端末共通鍵とを受け取る。受け取った端末共通鍵を用いて受け取った暗号化パスワード、暗号化入力データ、暗号化現パスワード及び暗号化新パスワードに復号アルゴリズム D1 を施して、パスワードを生成し、生成したパスワードを制御部 607 へ出力する。

- 10 また、パスワードとサーバ共通鍵、入力データとサーバ共通鍵又は現パスワードと新パスワードとサーバ共通鍵とを受け取る。受け取ったサーバ共通鍵を用いて、受け取ったパスワード、入力データ、現パスワード及び新パスワードに暗号化アルゴリズム E3 を施して暗号化パスワード、暗号化入力データ、暗号化現パスワード及び暗号化新パスワードを生成し、生成した暗号化パスワード、暗号化入力データ、暗号化現パスワード及び暗号化新パスワードを制御部 607 へ出力する。

15 1. 5 パスワード変更システムの動作

パスワード変更システムの動作について以下に説明する。

(1) ユーザ端末 100 による処理

- 20 ユーザ端末 100 による処理について図 19～図 26 に示すフローチャートを用いて説明する。なお、具体的には図示していないが、以下の動作において、機器間の各種情報の送受信の際には、処理を実行するアプリサーバ 200 又は管理サーバ 600 のアプリ番号とユーザ端末 100 の端末 ID が各種情報と共に送受信される。

- 25 ユーザ端末 100 は、利用者のボタン操作を受け付け（ステップ S101）、電子申請を示すボタン操作を受け付けると、ステップ S102 へ処理を移す。その他の処理を示すボタン操作を受け付けると、その他の処理を行う（ステップ S100）。

ユーザ端末 100 は、管理サーバ 600 と相互認証を行い端末共通鍵を共有する（ステップ S102）。

ユーザ端末 100 との相互認証が完了すると、管理サーバ 600 は、

ログイン画面データを読み出し（ステップS103）、読み出したログイン画面データを、ユーザ端末100へ送信する（ステップS104）。

ユーザ端末100は、管理サーバ600からログイン画面データを受信し、受信したログイン画面データからログイン画面151を生成しモニタに表示する（ステップS105）。次に、利用者によるユーザIDとパスワードの入力を受け付け（ステップS107）、受け付けたパスワードを、端末共通鍵を用いて暗号化し暗号化パスワードを生成する（ステップS108）。ユーザIDと生成した暗号化パスワードとを、インターネット20を介して管理サーバ600へ送信する（ステップS109）。

10 管理サーバ600は、インターネット20を介してユーザIDと暗号化パスワードとを受け取り、受け取った暗号化パスワードを端末共通鍵を用いて復号し、パスワードを生成する（ステップS111）。次に、パスワードテーブル621内で受け取ったユーザIDとパスワードを含むパスワード情報の有無を確認し（ステップS112）、受け取ったユーザIDとパスワードを含むパスワード情報が存在しなければ、認証失敗と判断し（ステップS113のNO）、ステップS103から処理をやり直す。受け取ったユーザIDとパスワードを含むパスワード情報が存在すれば、認証成功と判断し（ステップS113のYES）、受け取ったユーザIDとパスワードを含むパスワード情報と受信したユーザ端末100
15 IDとパスワードを含むパスワード情報が存在しなければ、認証失敗と判断し（ステップS113のNO）、ステップS103から処理をやり直す。受け取ったユーザIDとパスワードを含むパスワード情報が存在すれば、認証成功と判断し（ステップS113のYES）、受け取ったユーザIDとパスワードを含むパスワード情報と受信したユーザ端末100
20 の端末IDとを基に、ログイン情報632を生成しログインテーブル631に追加して書き込む（ステップS115）。

次に、情報記憶部610からメニュー画面データを読み出し、読み出したメニュー画面データと、ログインテーブル631に追加したログイン情報632とを基に端末用メニュー画面データを生成し（ステップS116）、生成した端末用メニュー画面データをインターネット20を介して、ユーザ端末100へ送信する（ステップS117）。

25 ユーザ端末100は、インターネット20を介して端末用メニュー画面データを受信し、受信した端末用メニュー画面データからメニュー画面161を生成し、モニタに表示する（ステップS121）。次に、利用

者によるメニューの選択を受け付ける（ステップS122）。

利用者のボタン操作により、パスワード変更が選択されると（ステップS122）、パスワード変更処理へ移行する（ステップS127）。

利用者により、出張費精算が選択されると（ステップS122）、アプリ番号「001」を読み出す（ステップS123）。利用者により、休暇申請が選択されると（ステップS122）、アプリ番号「002」を読み出す（ステップS124）。利用者により、会議室予約が選択されると（ステップS122）、アプリ番号「003」を読み出す（ステップS125）。利用者により、従業員購入が選択されると（ステップS122）、アプリ番号「004」を読み出す（ステップS126）。次に、読み出したアプリ番号とサービス開始要求を管理サーバ600へ送信する（ステップS128）。

管理サーバ600は、インターネット20を介してユーザ端末100からアプリ番号とサービス開始要求とを受信する。サービス開始要求とともに受信した端末IDを含むログイン情報632を選択し、選択したログイン情報632に含まれる処理状況が「通常」であるか否かを確認する（ステップS131）。処理状況が「通常」でないと判断すると（ステップS131のNO）、情報記憶部610からwaitメッセージを読み出し（ステップS146）、読み出したwaitメッセージを、インターネット20を介してユーザ端末100へ送信する（ステップS147）。

ユーザ端末100は、管理サーバ600から、waitメッセージを受信し、受信したwaitメッセージを表示する（ステップS148）。

選択したログイン情報632の処理状況が「通常」であると判断すると（ステップS131のYES）、次に、受信したアプリ番号を判別し（ステップS132）、アプリ番号が「002」であると判断すると（ステップS132の002）、第2アプリサーバ200bとの通信を開始する。アプリ番号が「003」であると判断すると（ステップS132の003）、第3アプリサーバ200cとの通信を開始する。アプリ番号が「004」であると判断すると（ステップS132の004）、第4アプリサ

サーバ200dとの通信を開始する（ステップS135）。

5 アプリ番号が「001」とであると判断すると（ステップS132の001）、第1アプリサーバ200aとの通信を開始する。先ず、管理サーバ600は、第1アプリサーバ200aと相互認証を行いサーバ共通鍵を共有する（ステップS136）。

次に、選択したログイン情報632に含まれるユーザIDとパスワードを読み出し（ステップS139）、読み出したパスワードをサーバ共通鍵を用いて暗号化して、暗号化パスワードを生成する（ステップS141）。受信したサービス開始要求とアプリ番号「001」と読み出したユーザIDと生成した暗号化パスワードとを第1アプリサーバ200aへ送信する（ステップS142）。

10 第1アプリサーバ200aは、インターネット20を介して管理サーバ600から、サービス開始要求とアプリ番号「001」とユーザIDと暗号化パスワードとを受信し、サーバ共通鍵を用いて、受信した暗号化パスワードを復号しパスワードを生成する（ステップS151）。パスワードテーブル221内で、受信したユーザIDと生成したパスワードとを含むパスワード情報の有無を確認し（ステップS152）、受信したユーザIDと生成したパスワードとを含むパスワード情報が存在しなければ、認証失敗と判断し（ステップS153のNO）、管理サーバ600の記憶しているパスワードと第1アプリサーバ200aの記憶しているパスワードとが一致していないことを示すパスワードエラー信号と、受信したユーザIDとをインターネット20を介して管理サーバ600へ送信する（ステップS166）。

25 管理サーバ600は、第1アプリサーバ200aからパスワードエラー信号とユーザIDとを受信し、端末用強制終了画面データを生成し（ステップS167）、生成した端末用強制終了画面データをユーザ端末100へ送信する（ステップS168）。次に、管理サーバ600は、エラー画面331を生成し（ステップS169）、生成したエラー画面を表示部613へ表示しパスワードの不一致の発生を操作者に知らせる（ステッ

プ S 1 7 1)。

ユーザ端末 1 0 0 は、インターネット 2 0 を介して、管理サーバ 6 0 0 から端末用強制終了画面データを受信し、受信した端末用強制終了画面データから強制終了画面 3 2 1 を生成し、生成した強制終了画面 3 2 1 をモニタに表示し (ステップ S 1 7 2)、処理を終了する。

パスワードテーブル 2 2 1 内に、受信したユーザ ID と生成したパスワードとを含むパスワード情報 2 2 3 が存在すると、第 1 アプリサーバ 2 0 0 a は、認証成功と判断し (ステップ S 1 5 3 の YES)、パスワード情報 2 2 3 とサービス開始要求と共に受信した端末 ID とを基に、ログイン情報 2 3 2 を生成し、生成したログイン情報 2 3 2 をアプリログインテーブル 2 3 1 に追加して書き込む (ステップ S 1 5 4)。

次に、第 1 アプリサーバ 2 0 0 a は、端末用精算画面データを生成し (ステップ S 1 5 5)、生成した端末用精算画面データを管理サーバ 6 0 0 へ送信する (ステップ S 1 5 6)。

15 管理サーバ 6 0 0 は、インターネット 2 0 を介して、第 1 アプリサーバ 2 0 0 a から端末用精算画面データを受信し、受信した端末用精算画面データをユーザ端末 1 0 0 へ送信する (ステップ S 1 5 8)。

ユーザ端末 1 0 0 は、インターネット 2 0 を介して、管理サーバ 6 0 0 から端末用精算画面データを受信し、受信した端末用精算画面データから精算画面 1 7 1 を生成し、モニタに表示する (ステップ S 1 5 9)。

次に、利用者によるデータの入力を受け付け (ステップ S 1 6 1)、端末共通鍵を用いて受け付けた入力データを暗号化し、暗号化入力データを生成する (ステップ S 1 6 2)。次に、生成した暗号化入力データを、管理サーバ 6 0 0 へ送信する (ステップ S 1 7 6)。

25 管理サーバ 6 0 0 は、インターネット 2 0 を介して、ユーザ端末 1 0 0 から暗号化入力データを受信し (ステップ S 1 7 7)、受信した暗号化入力データを端末共通鍵を用いて復号し、入力データを生成する (ステップ S 1 7 7)。次に、サーバ共通鍵を用いて、生成した入力データを暗号化して暗号化入力データを生成し (ステップ S 1 7 9)、生成した暗号

化入力データを第1アプリサーバ200aへ送信する(ステップS181)。

5 第1アプリサーバ200aは、インターネット20を介して暗号化入力データを受信し、サーバ共通鍵を用いて受信した暗号化入力データを復号し、入力データを生成する(ステップS182)。次に、生成した入力データを基に、出張費精算処理を行う(ステップS183)。出張費精算処理が終わると、第1アプリサーバ200aは、端末用精算終了画面データを生成し(ステップS184)、生成した端末用精算終了画面データを管理サーバ600へ送信する(ステップS186)。

10 管理サーバ600は、インターネット20を介して、第1アプリサーバ200aから端末用精算終了画面データを受信し、受信した端末用精算終了画面データをユーザ端末100へ送信する(ステップS188)。

ユーザ端末100は、インターネット20を介して管理サーバ600から端末用精算終了画面データを受信し、受信した端末用精算終了画面データから精算終了画面181を生成し、モニタに表示する(ステップS191)。次に、利用者によるボタン操作を受け付け(ステップS192)、メニューボタン182の押下を受け付けると、ステップS121に戻りメニューの選択を受け付ける。

20 ログアウトボタン183の押下を受け付けると(ステップS192)、ユーザ端末100は、ログアウトを示すログアウト通知を管理サーバ600へ送信する(ステップS193)。

25 管理サーバ600は、インターネット20を介してユーザ端末100からログアウト通知を受信し、受信したログアウト通知を第1アプリサーバ200aに送信する(ステップS194)。次に、ログアウト通知ト
供に受信した端末IDを含むログイン情報632を選択し、選択したログイン情報632をログインテーブル631から削除する(ステップS195)。また、図示していないが、第2アプリサーバ200b～第3アプリサーバ200dへも同様にログアウト通知を送信する。

第1アプリサーバ200aは、インターネット20を介して管理サー

5 パ600からログアウト通知を受信する。ログアウト通知と共に受信した端末IDを含むログイン情報を検索し、受信した端末IDを含むログイン情報232が存在すれば、ログイン情報232をアプリログインテーブル231から削除する(ステップS196)。第2アプリサーバ200b～第4アプリサーバ200dにおいても、同様にして自身の記憶しているアプリログインテーブル上に、受信した端末IDを含むログイン情報が存在すれば、削除する。

(2) 管理サーバ600によるパスワード変更処理

10 管理サーバ600によるパスワード変更処理について、図27～図29のフローチャートを用いて説明する。これは、図20のステップS127の詳細である。

ユーザ端末100は、アプリ番号「005」を読み出し(ステップS300)、読み出したアプリ番号「005」とパスワード変更指示を管理サーバ600へ送信する(ステップS301)。

15 管理サーバ600は、インターネット20を介して、アプリ番号「005」とパスワード変更指示を受信する。パスワード変更指示を受信すると、端末用パスワード変更画面データを生成し(ステップS302)、生成した端末用パスワード変更画面データをユーザ端末100へ送信する(ステップS303)。

20 ユーザ端末100は、インターネット20を介して、管理サーバ600から端末用パスワード変更画面データを受信し、受信した端末用パスワード変更画面データからパスワード変更画面191を生成し、モニタに表示する(ステップS304)。次に、利用者による現パスワードと新パスワードの入力を受け付ける(ステップS306)。端末共通鍵を用いて、受け付けた現パスワードと新パスワードとを暗号化し、暗号化現パスワードと暗号化新パスワードとを生成する(ステップS307)。次に、生成した暗号化現パスワードと暗号化新パスワードとを、管理サーバ600へ送信する(ステップS308)。

管理サーバ600は、インターネット20を介して、ユーザ端末100

0 から暗号化現パスワードと暗号化新パスワードとを受信する。暗号化現パスワードと暗号化新パスワードと供に受信した端末 I D を基に、ログインテーブル 6 3 1 内のログイン情報 6 3 2 を選択し、選択したログイン情報 6 3 2 の処理状況を「パスワード変更中」に書き換える（ステップ S 3 0 9）。

次に、端末共通鍵を用いて、受信した暗号化現パスワードと暗号化新パスワードを復号し、現パスワードと新パスワードとを生成する（ステップ S 3 1 1）。書き換えたログイン情報 6 3 2 に含まれるユーザ I D を読み出し（ステップ S 3 1 2）、パスワードテーブル 6 2 1 内で、読み出したユーザ I D と生成した現パスワードとを含むパスワード情報の有無を確認する（ステップ S 3 1 3）。

パスワードテーブル 6 2 1 内に、読み出したユーザ I D と生成した現パスワードとを含むパスワード情報が、存在しなければ、認証が失敗であると判断し（ステップ S 3 1 6 の N O）、ステップ S 3 0 2 へ戻り、再度、端末用パスワード変更画面データを送信する。

パスワードテーブル 6 2 1 内に、読み出したユーザ I D と生成した現パスワードとを含むパスワード情報が、存在すれば、認証が成功であると判断する（ステップ S 3 1 6 の Y E S）。

次に、読み出しユーザ I D と生成した現パスワードとを含むパスワード変更情報 6 5 2 をパスワード変更テーブル 6 5 1 から選択し（ステップ S 3 1 7）、選択したパスワード変更情報 6 5 2 に含まれる現パスワードと新パスワードとを生成した現パスワードと新パスワードとに書き換える（ステップ S 3 1 8）。

次に、第 1 アプリサーバ 2 0 0 a のパスワード変更処理を行い（ステップ S 3 1 9）、これが正常に終了すると、第 2 アプリサーバ 2 0 0 b のパスワード変更処理を行い（ステップ S 3 2 1）、正常に終了しなければ図 3 2 に示すパスワード復旧処理のステップ S 3 6 4 へ処理を移す。第 2 アプリサーバ 2 0 0 b のパスワード変更が正常に終了すると、第 3 アプリサーバ 2 0 0 c のパスワード変更を行い（ステップ S 3 2 2）、正常

に終了しなければ図 3 2 のステップ S 3 6 3 へ処理を移す。第 3 アプリサーバ 2 0 0 c のパスワード変更が正常に終了すると、第 4 アプリサーバ 2 0 0 d のパスワード変更を行い (ステップ S 3 2 3)、正常に終了しなければ、図 3 2 のステップ S 3 6 2 へ処理を移す。第 4 アプリサーバ 2 0 0 d のパスワード変更が正常に終了しなければ、図 3 2 のステップ S 3 6 1 へ処理を移す。

第 1 アプリサーバ 2 0 0 a ~ 第 4 アプリサーバ 2 0 0 d のパスワード変更が全て正常に終了すると、管理サーバ 6 0 0 は、パスワードテーブル 6 2 1 から送信したユーザ ID を含むパスワード情報を選択し、選択したパスワード情報に含まれるパスワードを新パスワードに書き換る。また、ログインテーブル 6 3 1 から送信したユーザ ID を含むログイン情報 6 3 2 を選択し、選択したログイン情報 6 3 2 に含まれるパスワードを新パスワードに書き換える (ステップ S 3 2 6)。

次に、端末用変更完了画面データを生成し (ステップ S 3 2 7)、生成した端末用変更完了画面データをユーザ端末 1 0 0 へ送信し (ステップ S 3 2 8)、ログイン情報 6 3 2 の処理状況を「通常」に書き換える (ステップ S 3 2 9)。

ユーザ端末 1 0 0 は、インターネット 2 0 を介して、管理サーバ 6 0 0 から端末用変更完了画面データを受信し、受信した端末用変更完了画面データから変更完了画面 3 0 1 生成し、生成した変更完了画面 3 0 1 をモニタに表示する (ステップ S 3 3 1)。次に、利用者によるボタン操作を受け付け (ステップ S 3 3 2)、メニューボタン 3 0 2 の押下を受け付けると、ステップ S 1 2 1 へ戻り、メニュー画面を表示する。

ログアウトボタン 3 0 3 の押下を受け付けると、管理サーバ 6 0 0 へログアウト通知を送信し、処理を終了する (ステップ S 3 3 3)。

管理サーバ 6 0 0 は、インターネット 2 0 を介して、ユーザ端末 1 0 0 からログアウト通知を受信する。受信したログアウト通知を第 1 アプリサーバ 2 0 0 a ~ 第 4 アプリサーバ 2 0 0 d へ送信する (ステップ S 3 3 6)。次に、ログアウト通知と共に受信した端末 ID を基に、ログイ

ン情報 6 3 2 を選択し、選択したログイン情報 6 3 2 を消去する（ステップ S 3 3 4）。

5 アプリサーバ 2 0 0 は、管理サーバ 6 0 0 からログアウト通知を受信し、ログアウト通知と共に受信した端末 I D を含むログイン情報をアプリログインテーブル 2 3 1 内で検索し、受信した端末 I D を含むログイン情報を含むログイン情報が存在すれば、そのログイン情報を削除する（ステップ S 3 3 7）。

（3）アプリサーバ 2 0 0 のパスワード変更処理

10 各アプリサーバ 2 0 0 のパスワード変更処理について、図 3 0 ～ 3 1 に示すフローチャートを用いて説明する。なお、これは、図 2 8 のステップ S 3 1 9、ステップ S 3 2 1、ステップ S 3 2 2 及びステップ S 3 2 3 の詳細である。

15 管理サーバ 6 0 0 は、アプリサーバ 2 0 0 と相互認証を行いサーバ共通鍵を生成する（ステップ S 3 4 1）。ステップ S 3 1 8 において書き換えたパスワード変更情報 6 5 2 から、ユーザ I D と現パスワードと新パスワード抽出し、サーバ共通鍵を用いて、抽出した現パスワードと新パスワードとを暗号化し、暗号化現パスワードと暗号化新パスワードとを生成する（ステップ S 3 4 2）。抽出したユーザ I D と生成した暗号化現パスワードと暗号化新パスワードとをアプリサーバ 2 0 0 へ送信し、パスワード変更を指示する（ステップ S 3 4 3）。次に、パスワード変更指示を送信してからの経過時間を計測する t i m e カウンタを 0 に設定し、経過時間の計測を開始する（ステップ S 3 4 4）。

25 アプリサーバ 2 0 0 は、インターネット 2 0 を介して管理サーバ 6 0 0 から、ユーザ I D と暗号化現パスワードと暗号化新パスワードとを受信し、暗号化を指示される。サーバ共通鍵を用いて、受信した暗号化現パスワードと暗号化新パスワードとを復号し、現パスワードと新パスワードとを生成する（ステップ S 3 4 5）。

、パスワードテーブル 2 2 1 内で受信したユーザ I D を含むパスワード情報 2 2 3 を選択し、選択したパスワード情報 2 2 3 に含まれるパsw

ードを新パスワードに書き換える（ステップS346）。パスワードの書き換えが成功であると判断すると（ステップS347のYES）、終了信号「1」を生成する（ステップS349）。パスワードの書き換えが失敗であると判断すると（ステップS347のNO）、終了信号「0」を生成する（ステップS348）。5

次に、生成した終了信号を、インターネット20を介して、管理サーバ600へ送信する（ステップS351）。

管理サーバ600は、アプリサーバ200から終了信号を受信すると（ステップS355のYES）、受信した終了信号を判別し（ステップS356）、終了信号「1」であると判断すると、アプリサーバ200のパスワード変更を終了する。10

終了信号「0」であると判断すると（ステップS356の「0」）、パスワード復旧処理へ移行する（ステップS359）。

アプリサーバ200から、終了信号を受信していなければ（ステップS355のNO）、timeカウンタの値と最大待ち時間とを比較し（ステップS358）、timeカウンタが最大待ち時間を超えていないと判断すると（ステップS358のNO）、ステップS355へ戻り、アプリサーバ200から終了信号を受信するかtimeカウンタが最大待ち時間を超えるまで、ステップS355～ステップS358の処理を繰り返す。15
20

timeカウンタが最大待ち時間を超えていると判断すると（ステップS358のYES）、アプリサーバ200のパスワード変更が失敗あると判断し、パスワード復旧処理を行う（ステップS359）。

（4）管理サーバ600によるパスワード復旧処理

25 管理サーバ600によるパスワード復旧の処理について、図32のフローチャートを用いて説明する。これは、図31のステップS359の詳細である。

ただし、図28のステップS319の処理中であればステップS364からパスワード復旧処理を開始する。ステップS321の処理中であ

れば、ステップS 3 6 3からパスワード復旧処理を開始し、ステップS 3 2 2の処理中であれば、ステップS 3 6 2から、パスワード復旧の処理を開始する。図2 8のステップS 3 2 3の処理中であれば、ステップS 3 6 1からパスワード復旧の処理を開始する。

5 管理サーバ6 0 0は、第3アプリサーバ2 0 0 cのパスワード復旧を行い（ステップS 3 6 1）、これが正常に終了すれば、第2アプリサーバ2 0 0 bのパスワード復旧を行う（ステップS 3 6 2）。ステップS 3 6 2が正常に終了すれば、第1アプリサーバ2 0 0 aのパスワード復旧を行う（ステップS 3 6 3）。

10 ステップS 3 6 4が正常に終了すると、管理サーバ6 0 0は、変更失敗画面とログイン情報6 3 2とを基に、端末用変更失敗画面データを生成し（ステップS 3 6 4）、生成した端末用変更失敗画面データをユーザ端末1 0 0へ送信する（ステップS 3 6 6）。

ユーザ端末1 0 0は、インターネット2 0を介して、管理サーバ6 0
15 0から端末用変更失敗画面データを受信し、受信した端末用変更失敗画面データから変更失敗画面3 1 1を生成し、生成した変更失敗画面3 1 1をモニタに表示する（ステップS 3 6 7）。次に、利用者のボタン操作を受け付け（ステップS 3 6 8）、メニューボタン3 1 2の選択を受け付けると、ステップS 1 2 1へ処理を移す。

20 ログアウトボタン3 1 3の選択を受け付けると、管理サーバ6 0 0へログアウト通知を送信する（ステップS 3 7 1）。

管理サーバ6 0 0は、インターネット2 0を介してユーザ端末1 0 0
25 からログアウト通知を受信し、ログアウト通知と共に受信した端末IDを基に、ログイン情報6 3 2を選択し、選択したログイン情報6 3 2を削除する（ステップS 3 7 2）。

また、具体的には図示していないが、受信したログアウト通知をアプリサーバ2 0 0へ送信する。アプリサーバ2 0 0は、インターネット2 0を介して管理サーバ6 0 0からログアウト通知を受信し、ログアウト通知と共に受信した端末IDを含むログイン情報をアプリログインター

ブル 2 3 1 内で検索し、端末 I D を含むログイン情報が存在すれば、該当するログイン情報を削除する。

(5) アプリサーバ 2 0 0 のパスワード復旧処理

5 アプリサーバ 2 0 0 のパスワード復旧処理について、図 3 3 に示すフローチャートを用いて説明する。これは、図 3 2 のステップ S 3 6 1、ステップ S 3 6 2、ステップ S 3 6 3 の詳細である。

10 管理サーバ 6 0 0 は、パスワード復旧指示の送信回数をカウントする回数カウンタを 0 に設定する (ステップ S 3 8 0)。次に、パスワード変更情報 6 5 2 に含まれる、ユーザ I D と現パスワードと新パスワードと読み出し、サーバ共通鍵を用いて、読み出した現パスワードと新パスワードとを暗号化し、暗号化現パスワードと暗号化新パスワードとを生成する (ステップ S 3 8 1)。次に、読み出しユーザ I D と生成した暗号化現パスワードと暗号化新パスワードとをアプリサーバ 2 0 0 へ送信しパスワード復旧を指示する (ステップ S 3 8 2)。次に、パスワード復旧指示を送信してからの経過時間を計測する t i m e カウンタを 0 に設定し、経過時間の計測を開始する (ステップ S 3 8 3)

20 アプリサーバ 2 0 0 は、インターネット 2 0 を介して管理サーバ 6 0 0 から、ユーザ I D と暗号化現パスワードと暗号化新パスワードとを受信し、パスワード復旧の指示を受け取る。サーバ共通鍵を用いて受信した暗号化現パスワードと暗号化新パスワードとを復号し、現パスワードと新パスワードとを生成する (ステップ S 3 8 4)。次に、パスワードテーブル 2 2 1 上で受信したユーザ I D と生成した新パスワードとを含むパスワード情報を選択し、選択したパスワード情報のパスワードを現パスワードに書き換える (ステップ S 3 8 5)。

25 パスワードの書き換えが成功であれば (ステップ S 3 8 6 の Y E S)、終了通知「1」を生成する (ステップ S 3 8 7)。パスワードの書き換えが失敗であれば (ステップ S 3 8 6 の N O)、終了信号「0」を生成する (ステップ S 3 8 8)。次に、生成した終了信号を管理サーバ 6 0 0 へ送信する (ステップ S 3 8 9)。

管理サーバ600は、インターネット20を介して、アプリサーバ200から終了信号を受信すると(ステップS391のYES)、受信した終了信号を判別し(ステップS392)、終了信号「1」であると判断すると、これをもって、アプリサーバ200のパスワード復旧を正常に終了する。

終了信号「0」であると判断すると(ステップS392)、ステップS396へ処理を移す。

アプリサーバ200から、終了信号を受信していなければ(ステップS391のNO)、timeカウンタの値と最大待ち時間とを比較し(ステップS394)、timeカウンタが最大待ち時間を超えていないと判断すると(ステップS394のNO)、ステップS391へ戻り、アプリサーバ200から終了信号を受信するかtimeカウンタが最大待ち時間を超えるまで、ステップS391～ステップS394の処理を繰り返す。

timeカウンタが最大待ち時間を超えていると判断すると(ステップS394のYES)、回数カウンタに1加算し(ステップS396)、次に回数カウンタの値と制限回数を比較し(ステップS397)、制限回数を超えていなければ(ステップS397のNO)、ステップS382へ処理を移す。

制限回数を超えていると判断すると(ステップS397のYES)、パスワード復旧の失敗であると判断し、端末用強制終了画面データを生成し(ステップS398)、生成した端末用強制終了画面データをユーザ端末100へ送信する(ステップS399)。

次に、エラー画面331を生成し(ステップS402)、生成したエラー画面を表示部613に表示する(ステップS403)。

ユーザ端末100は、インターネット20を介して、管理サーバ600から端末用強制終了画面データを受信する。受信した端末用強制終了画面データから強制終了画面321を生成し、モニタに表示し(ステップS401)、処理を終了する。

(6) 相互認証処理

機器間での相互認証の動作について図35～図36を用いて説明する。

なお、この相互認証の方法は一例であり、他の認証方法、鍵共有方法を用いてもよい。また、相互認証は、ユーザ端末100と管理サーバ600の間又は管理サーバ600とアプリサーバ200の間で行うため、ここでは双方の機器を、機器A及び機器Bとして説明する。上記の説明では、ユーザ端末100と管理サーバ600の間の相互認証により生成される共通鍵を端末共通鍵、管理サーバ600とアプリサーバ200の間の相互認証により生成される共通鍵をサーバ共通鍵と呼称している。

ここで、 $Gen()$ を鍵生成関数とし、 Y をシステム固有のパラメータとする。鍵生成関数 $Gen()$ は、 $Gen(x, Gen(z, Y)) = Gen(z, Gen(x, Y))$ の関係を満たすものとする。鍵生成関数は任意の公知技術で実施可能なため、詳細についてここでは説明しない。

機器Aは、公開鍵証明書 $Cert_A$ を読み出し(ステップS201)、読み出した公開鍵証明書 $Cert_A$ を機器Bへ送信する(ステップS202)。

公開鍵証明書 $Cert_A$ を受信した機器Bは、認証局の公開鍵 PK_CA を用いて、公開鍵証明書 $Cert_A$ に含んで受信した認証局の署名データ Sig_CA に署名検証アルゴリズム V を施して署名検証する(ステップS203)。ここで、署名検証アルゴリズム V は、署名生成アルゴリズム S により生成された署名データを検証するアルゴリズムである。署名検証の結果が失敗であれば(ステップS204のNO) 処理を終了する。

署名検証の結果が成功であれば(ステップS204のYES)、機器Bは、CRLを読み出し(ステップS205)、公開鍵証明書 $Cert_A$ に含んで受信したID番号 ID_A が読み出したCRLに登録されているか否かを判断する(ステップS206)。登録されていると判断すると(ステップS206のYES)、処理を終了する。

登録されていないと判断すると(ステップS206のNO)、機器Bは、

公開鍵証明書 $Cert_B$ を読み出し (ステップ $S207$)、読み出した公開鍵証明書 $Cert_B$ を機器 A に送信する。

- 5 公開鍵証明書 $Cert_B$ を受信した機器 A は、認証局の公開鍵 PK_CA を用いて、公開鍵証明書 $Cert_B$ に含んで受信した認証局の署名データ Sig_CA に署名検証アルゴリズム V を施して署名検証する (ステップ $S209$)。署名検証の結果が失敗であれば (ステップ $S210$ の NO) 処理を終了する。

- 10 署名検証の結果が成功であれば (ステップ $S210$ の YES)、機器 A は、 CRL を読み出し (ステップ $S211$)、公開鍵証明書 $Cert_B$ に含んで受信した ID 番号 ID_B が読み出した CRL に登録されているか否かを判断する (ステップ $S212$)。登録されていると判断すると (ステップ $S212$ の YES)、処理を終了する。登録されていないと判断すると (ステップ $S212$ の NO)、処理を継続する。

- 15 機器 B は、乱数 Cha_B を生成し (ステップ $S213$)、生成した乱数 Cha_B を機器 A に送信する (ステップ $S214$)。

機器 A は、乱数 Cha_B を受信し、機器 A の秘密鍵 SK_A を用いて、受信した乱数 Cha_B に署名生成アルゴリズム S を施して署名データ Sig_A を生成し (ステップ $S215$)、生成した署名データ Sig_A を機器 B へ送信する (ステップ $S216$)。

- 20 機器 B は、署名データ Sig_A を受信すると、公開鍵証明書 $Cert_A$ に含んで受信した機器 A の公開鍵 PK_A を用いて、受信した署名データ Sig_A に、署名検証アルゴリズム V を施して署名検証する (ステップ $S217$)。署名検証の結果が失敗であると判断すると (ステップ $S218$ の NO) 処理を終了する。署名検証の結果が成功であると判断すると (ステップ $S218$ の YES)、処理を続ける。

25 機器 A は、乱数 Cha_A を生成し (ステップ $S219$)、生成した乱数 Cha_A を機器 A に送信する (ステップ $S220$)。

機器 B は、乱数 Cha_A を受信し、機器 B の秘密鍵 SK_B を用いて、受信した乱数 Cha_A に署名生成アルゴリズム S を施して署名デ

ータ Sig_B を生成し (ステップ $S221$)、生成した署名データ Sig_B を機器 A へ送信する (ステップ $S222$)。

機器 A は、署名データ Sig_B を受信すると、公開鍵証明書 $Cert_B$ に含んで受信した機器 B の公開鍵 PK_B を用いて、受信した署名データ Sig_B に、署名検証アルゴリズム V を施して署名検証する (ステップ $S223$)。署名検証の結果が失敗であると判断すると (ステップ $S224$ の NO) 処理を終了する。署名検証の結果が成功であると判断すると (ステップ $S224$ の YES)、次に、乱数「 a 」を生成し (ステップ $S225$)、生成した乱数「 a 」を用いて $Key_A = Gen(a, Y)$ を生成し (ステップ $S226$)、生成した Key_A を機器 B へ送信する (ステップ $S227$)。

機器 B は、 Key_A を受信すると、乱数「 b 」を生成し (ステップ $S228$)、生成した乱数「 b 」を用いて $Key_B = Gen(b, Y)$ を生成し (ステップ $S229$)、生成した Key_B を機器 A へ送信する (ステップ $S230$)。

また、生成した乱数「 b 」と受信した Key_A とを用いて、 $Key_AB = Gen(b, Key_A) = Gen(b, Gen(a, Y))$ を生成し、これを共通鍵とする (ステップ $S231$)。

機器 A は、 Key_B を受信し、生成した乱数「 a 」と受信した Key_B とから $Key_AB = Gen(a, Key_B) = Gen(a, Gen(b, Y))$ を生成し、これを共通鍵とする (ステップ $S232$)。

(7) パスワード変更の実行例

以下に、パスワード変更の 1 実行例を図 37 を用いて説明する。ここでは、ユーザ ID 「 $maeda$ 」の利用者の現パスワード「 $ozy12$ 」を新パスワード「 $nwy56$ 」に変更する。ユーザ端末 100 と管理サーバ 600 間の通信及び管理サーバ 600 とアプリサーバ 200 間の通信において、現パスワード及び新パスワードは、端末共通鍵又はサーバ共通鍵を用いた秘密通信により安全に送受信されるが、以下の説明において、簡略化のため、暗号化及び復号の処理についての説明を省略する。

変更前の各アプリサーバ200は、図37(a)に示すようにユーザID「maeda」に対応するパスワード「ozy12」を記憶している。

ユーザ端末100からのパスワード変更指示により、管理サーバ600は、ユーザ端末100へ端末用パスワード変更画面データを送信する。

ユーザ端末100は、端末用パスワード変更画面データを受信し、受信した端末用パスワード変更画面データからパスワード変更画面191生成し表示する。利用者による現パスワード「ozy12」と新パスワード「nwy56」の入力を受け付け、受け付けた現パスワード「ozy12」と新パスワード「nwy56」を、管理サーバ600へ送信する。

管理サーバ600は、ユーザ端末100から現パスワード「ozy12」と新パスワード「nwy56」を受信する。次に、第1アプリサーバ200aへ受信した現パスワード「ozy12」と新パスワード「nwy56」とを送信しパスワードの変更を指示する。

第1アプリサーバ200aは、自身の記憶している現パスワード「ozy12」を新パスワード「nwy56」に書き換え、終了信号「1」を送信する。

第1アプリサーバ200aから、正常にパスワード変更が終了したことを示す終了信号「1」を受信すると、管理サーバ600は、第2アプリサーバ200bにも同様に現パスワード「ozy12」と新パスワード「nwy56」とを送信しパスワードの変更を指示し、終了信号「1」を受信する。このとき、第1アプリサーバ200a及び第2アプリサーバ200bは、図37bに示すように、新パスワード「nwy56」を記憶しており、第3アプリサーバ200cと第4アプリサーバ200dは、現パスワード「ozy12」を記憶している。

管理サーバ600は、次に、第3アプリサーバ200cに現パスワード「ozy12」と新パスワード「nwy56」とを送信しパスワードの変更を指示する。

ここで、第3アプリサーバ200cは、パスワードの変更を失敗し、終了信号「0」を管理サーバ600へ送信する。

第3アプリサーバ200cから、パスワードの変更が失敗であることを示す終了信号「0」を受け取ると、管理サーバ600は、第2アプリサーバ200bへ現パスワード「ozy12」と新パスワード「nwy56」とを送信しパスワードの復旧を指示する。次に、管理サーバ600は、第2アプリサーバ200bから、パスワードの復旧が成功したことを示す終了信号「1」を受け取る。次に、第1アプリサーバ200aにも同様に、パスワード復旧を指示し、第1アプリサーバ200aから終了信号「1」を受け取る。これをもって、パスワードの復旧の完了とする。このとき、各アプリサーバは、図37(c)の示すように、現パスワード「ozy12」を記憶している。

図37(d)は、第3アプリサーバ200c及び第4アプリサーバ200dのパスワード変更が成功した場合に各アプリサーバが記憶しているパスワードを示している。

1. 6 まとめ

上記に、説明したように、本実施の形態によると、管理サーバ600は、ユーザ端末100から、パスワードの変更指示を受け取る。管理サーバ600は、端末秘密鍵を用いた秘密通信により、ユーザ端末100から安全に現パスワードと新パスワードとを受信する。

次に、サーバ共通鍵を用いた秘密通信により、安全に現パスワードと新パスワードとを第1アプリサーバ200aへ送信しパスワードの変更を指示する。第1アプリサーバ200aのパスワード変更が成功であれば、同様にして、第2アプリサーバ200a～第4アプリサーバ200dの順にパスワードの変更を指示する。

第1アプリサーバ200a～第4アプリサーバ200dのいずれかでパスワードの変更が失敗すると、既にパスワード変更が終了したアプリサーバに対して、現パスワードと新パスワードとを送信しパスワードの復旧を指示する。

このようにして、複数のアプリサーバのうちいずれかがパスワードの変更に失敗した場合でも、複数のアプリサーバのパスワードを統一することができる。

2. 実施の形態 2

5 以下に実施の形態 2 のパスワード変更システムについて、説明する。

パスワード変更システムは図 38 に示すように、ユーザ端末 100、内部ユーザ端末 150、160・・・、第 1 アプリサーバ 200a、第 2 アプリサーバ 200b、第 3 アプリサーバ 200c、第 4 アプリサーバ 200d、管理サーバ 600b 及びルータ 800 から構成される。

10 第 2 アプリサーバ 200b～第 4 アプリサーバ 200d 及び管理サーバ 600b は、バス 31 に接続されており、バス型 LAN を形成している。内部ユーザ端末 150、160・・・及び管理サーバ 600b は、バス 32 に接続されており、バス型 LAN を形成している。バス 31 及び 32 は、具体的には、両端に終端装置を備えた同軸ケーブルである。

15 管理サーバ 600b は、さらに、ファイアウォール機能を備えるルータ 800 を介してインターネットと接続されている。

管理サーバ 600b、第 2 アプリサーバ 200b～第 4 アプリサーバ 200d 及び内部ユーザ端末 150、160・・・は、一例として、同一の建物内の LAN を構成している。

20 ユーザ端末 100 と第 1 アプリサーバ 200a は、インターネット 20 に接続されている。

実施の形態 1 と同様に、管理サーバ 600b 及び第 1 アプリサーバ 200a～第 4 アプリサーバ 200d は、あらかじめ正当な利用者のユーザ ID とパスワードを対応付けて記憶している。

25 第 1 アプリサーバ 200a～第 4 アプリサーバ 200d は、それぞれ、出張費精算、休暇申請、会議室予約及び従業員購入のサービスを提供する。

利用者は、ユーザ端末 100 を用いて、インターネット 20 及び管理サーバ 600b を介して、これらのサービスを利用する。また、内部ユ

ーザ端末 150、160・・・を用いて、バス 31 及び 32 を介して、これらサービスを利用することもできる。

このとき、ユーザ端末 100 又内部ユーザ端末 150、160・・・は、管理サーバ 600b に利用者のユーザ ID とパスワードを送信する。

5 管理サーバ 600b 及び第 1 アプリサーバ 200a ～第 4 アプリサーバ 200d は、ユーザ端末 100 又内部ユーザ端末 150、160・・・から送信されたユーザ ID とパスワードを検証し、ユーザ端末 100 又内部ユーザ端末 150、160・・・の利用者が正当な利用者であることを認証し、各アプリサーバは、それぞれが備えるサービスを提供する。

10 また、管理サーバ 600b は、ユーザ端末 100 又内部ユーザ端末 150、160・・・からパスワード変更の指示と現在のパスワードと新しいパスワードとを受信する。管理サーバ 600b は、第 1 アプリサーバ 200a ～第 4 アプリサーバ 200d へ、受け取った新しいパスワードを順次送信し、パスワードの変更を指示する。

15 ここで、第 1 アプリサーバ 200a ～第 4 アプリサーバ 200d の何れかで、パスワードの変更が正常に行われなかった場合、管理サーバ 600b は、既にパスワード変更が終了しているアプリサーバに現在のパスワードを送信し、現在のパスワードへパスワードを変更し直すように指示する。

20 ユーザ端末 100、内部ユーザ端末 150、160・・・の具体的な構成及び動作は、実施の形態 1 のユーザ端末 100 と同一であるので説明を省略する。

第 1 アプリサーバ 200a ～第 4 アプリサーバ 200d の具体的な構成及び動作は、実施の形態 1 の第 1 アプリサーバ 200a ～第 4 アプリ
25 サーバ 200d と同一であるので説明を省略する。

管理サーバ 600b は、図 39 に示すように、送受信部 601b、認証部 603、パスワード変更部 606、制御部 607、暗号処理部 608、パスワード復旧部 614、変更判定部 609、変更結果通知部 615、情報記憶部 610、入力部 612 及び表示部 613 から構成される。

送受信部 601b は、バス 31、32 及びバス 35 と接続されている。
送受信部 601b は、バス 31 を介して、第 2 アプリサーバ 200b ~
第 4 アプリサーバ 200d と管理サーバ 600b 内の各部との間で情報の
送受信を行い、バス 32 を介して、内部ユーザ端末 150、160...
5 と管理サーバ 600b 内の各部との間で情報の送受信を行う。また、バス
35、ルータ 20 及びインターネット 20 を介してユーザ端末 100
及び第 1 アプリサーバ 200a と管理サーバ 600b 内の各部との間で、
情報の送受信を行う。

この際、第 2 アプリサーバ 200b ~ 第 4 アプリサーバ 200d との
10 情報の送受信においては、送受信部 601b は、バス 31 を選択し、内
部ユーザ端末 150、160... との情報の送受信においては、バス
32 を選択する。また、ユーザ端末 100 及び第 1 アプリサーバ 200
a との情報の送受信においては、バス 35 を選択する。

送受信部 601b のその他の具体的な動作は、実施の形態 1 の送受信
15 部 601 と同様である。

また、認証部 603、パスワード変更部 606、制御部 607、暗号
処理部 608、パスワード復旧部 614、変更判定部 609、変更結果
通知部 615、入力部 612、表示部 613 の具体的な動作及び情報記
憶部 610 の構成は、図 13 を用いて説明した実施の形態 1 と同様であ
20 る。

ルータ 800 は、ファイアウォール機能を備えており、インターネッ
ト 20 に接続された外部機器から、LAN 内の各機器宛に送信された各
種の情報の通過又は遮断を行う。具体的には、インターネットを介して
受信したパケットに含まれる、送信元及び送信先の IP アドレスやポー
25 ト番号が、あらかじめ設定された条件を満たしているか否かを判断し、
条件を満たしていれば通過させ、満たしていなければ受信したパケット
を削除する。このような方法は、一般的にパケットフィルタリングとい
われる。また、このファイアウォール機能は一例であり、他の方法を用
いてもよい。

以上に説明したように、本実施の形態では、ルータ 800 のファイアウォール機能により、インターネット 20 に接続された不正な外部機器による攻撃から管理サーバ 600 b 及び LAN に接続されている各機器を防御することができる。

5 3. 実施の形態 3

以下に実施の形態 3 のパスワード変更システムについて、説明する。

パスワード変更システムは、図 40 に示すように、ユーザ端末 170、180・・・、第 1 アプリサーバ 200 a ～第 4 アプリサーバ 200 d 及び管理サーバ 600 c から構成される。

10 第 1 アプリサーバ 200 a ～第 4 アプリサーバ 200 d 及び、管理サーバ 600 c はバス 33 に接続されておりバス型 LAN を形成している。ユーザ端末 170、180・・・と管理サーバ 600 c は、バス 34 に接続されており、バス型 LAN を形成している。バス 33 及び 34 は、具体的には、両端に終端装置を備える同軸ケーブルである。

15 管理サーバ 600 c、第 1 アプリサーバ 200 a ～第 4 アプリサーバ 200 d 及びユーザ端末 170、180・・・は、一例として、同一の建物内の LAN を構成している。

20 第 1 アプリサーバ 200 a ～第 4 アプリサーバ 200 d は、それぞれ、出張費精算、休暇申請、会議室予約及び従業員購入のサービスを提供する。

利用者は、ユーザ端末 170、180・・・のうち何れかを使用し、管理サーバ 600 c を介して第 1 アプリサーバ 200 a ～第 4 アプリサーバ 200 d の提供するサービスを利用する。

25 このとき、利用者の使用するユーザ端末 170 は、管理サーバ 600 c に利用者のユーザ ID とパスワードを送信する。

管理サーバ 600 c 及び第 1 アプリサーバ 200 a ～第 4 アプリサーバ 200 d は、ユーザ ID とパスワードを検証し、ユーザ端末 100 の利用者が正当な利用者であることを認証し、各アプリサーバ 200 は、それぞれが備えるサービスを提供する。

また、管理サーバ600cは、ユーザ端末170からパスワード変更の指示を受信し、ユーザ端末100から、現在のパスワードと新しいパスワードとを受信する。管理サーバ600cは、第1アプリサーバ200a～第4アプリサーバ200dへ、受け取った新しいパスワードを順次送信し、パスワードの変更を指示する。

ここで、第1アプリサーバ200a～第4アプリサーバ200dの何れかで、パスワードの変更が正常に行われなかった場合、管理サーバ600cは、既にパスワード変更が終了しているアプリサーバに現在のパスワードを送信し、現在のパスワードへパスワードを変更し直すように指示する。

第1アプリサーバ200a～第4アプリサーバ200dの具体的な構成及び動作はそれぞれ実施の形態1の第1アプリサーバ200a～第4アプリサーバ200dと同様であるので説明を省略する。

ユーザ端末170、180・・・の具体的な構成及び動作は実施の形態1のユーザ端末100と同様であるので説明を省略する。

管理サーバ600cは、図41に示すように、送受信部601c、認証部603、パスワード変更部606、制御部607、暗号処理部608、パスワード復旧部614、変更判定部609、変更結果通知部615、情報記憶部610、入力部612及び表示部613から構成される。

送受信部601cは、バス33を介して、第1アプリサーバ200a～第4アプリサーバ200dと管理サーバ600c内の各部との間で情報の送受信を行う。バス34を介してユーザ端末170、180・・・と管理サーバ600c内部の各部との間で情報の送受信を行う。

この際、第1アプリサーバ200a～第4アプリサーバ200dとの情報の送受信において、送受信部601cは、バス33を選択し、ユーザ端末170、180・・・との情報の送受信において、バス34を選択する。

送受信部601cの具体的な動作は、実施の形態1の送受信部601と同様である。

認証部 603、パスワード変更部 606、制御部 607、暗号処理部 608、パスワード復旧部 614、変更判定部 609、変更結果通知部 615、入力部 612 及び表示部 613 の具体的な動作、情報記憶部 610 の構成は実施の形態 1 の管理サーバ 600 と同様であるので説明を省略する。

本実施の形態では、アプリサーバ 200 は管理サーバ 600 c を介してユーザ端末 170、180 と接続されている。利用者が、ユーザ端末 170 及び 180 を使用して、アプリサーバ 200 の提供するサービスを利用する際に送受信される各種の情報は必ず管理サーバ 600 c を通過するため、管理サーバ 600 c は、悪意のある利用者による不正なサービスの利用を発見しやすくなる。

また、本実施の形態のように、閉じた LAN の場合又はファイアウォール等により保護された LAN 内のみで上述したサービス提供及びパスワード変更に係る通信を行う場合、認証部 603 による相互認証を省略することもできる。これにより、上述したサービス提供の処理及びパスワード変更の処理をより迅速に行うことができる。

4. その他の変形例

(1) 管理サーバによるパスワード変更開始

上記の実施の形態 1～3 において、ユーザ端末又は内部ユーザ端末からパスワード変更の要求を受信することにより、パスワード変更の処理を開始しているが、管理サーバ 600 から利用者にパスワードの変更を促してもよい。

具体的には、管理サーバ 600 は、あらかじめパスワードの最長使用期間を記憶している。また、利用者が主に使うユーザ端末の IP アドレスを、利用者のユーザ ID と対応付けて記憶している。パスワードテーブル 621 に代わって、パスワードテーブル 621 b を記憶している。

パスワードテーブル 621 b は、図 42 に示すように、複数のパスワード情報 622 b、623 b、624 b・・・から構成される。各パスワード情報は、ユーザ ID、氏名、パスワード及び更新日を含む。ユー

ザ I D、氏名及びパスワードは、上記の実施の形態のパスワードテーブル 6 2 1 に含まれるユーザ I D、氏名及びパスワードと同様であるので説明を省略する。更新日は、パスワード情報に含まれるパスワードが変更された最近の日付を示しており、例えばパスワード情報 6 2 2 b に含まれるパスワードは、2 0 0 年 5 月 1 0 日に「o z y 1 2」に変更されたことを示す。

管理サーバ 6 0 0 は、定期的に各パスワード情報に含まれる変更日をチェックし、最長使用期間を超えてパスワードの変更を行っていない利用者に対し、あらかじめ記憶しているユーザ端末へ、パスワードが最長使用期間を過ぎていることを通知するメッセージを送信し、パスワードの変更を促す。

(2) 強制パスワード変更

また上記の (1) において、最長使用期間を超えてパスワードを変更していない利用者が、各種サービスを利用しようとするときに、強制的にパスワード変更を促してもよい。

具体的には、上記の実施の形態 1 ~ 3 において、管理サーバ 6 0 0 は、ユーザ端末からユーザ I D と暗号化パスワードを受信すると、先ず、パスワードテーブル 6 2 1 b 内で受信したユーザ I D を含むパスワード情報 6 2 2 b を選択する。選択したパスワード情報 6 2 2 b に含まれる変更日を読み出す。読み出した更新日に、最長使用期間 (例えば 3 0 日) を加算した変更期限「2 0 0 0 . 6 . 9」を算出し、算出した変更期限「2 0 0 0 . 6 . 9」と現在の日付とを比較する。現在の日付が変更期限「2 0 0 0 . 6 . 9」を越えていると判断すると、管理サーバ 6 0 0 は、ユーザ端末に端末用パスワード変更画面データを送信し、パスワードの変更を行わなければ、サービスの利用ができないようにしてもよい。

(3) アプリサーバ 2 0 0 への問合せ

また、実施の形態 1 ~ 3 では、管理サーバ 6 0 0 は各アプリサーバ 2 0 0 にユーザ I D と暗号化現パスワードと暗号化新パスワードとパスワード変更指示とを同時に送信しているが、各アプリサーバ 2 0 0 にあ

かじめパスワードの変更が可能か否かを問合せ、全てのアプリサーバ200が、パスワード変更可能である場合にのみ、パスワード変更を指示するとしてもよい。

具体的には、管理サーバ600は、まず、第1アプリサーバ200aにユーザIDと暗号化現パスワードと暗号化新パスワードとを送信し、パスワード変更が可能か否かを問い合わせる。

第1アプリサーバ200aは、管理サーバ600からユーザIDと暗号化現パスワードと暗号化新パスワードを受信し、パスワード変更が可能か否かの問合せを受け付けると、パスワード変更が可能か否かを示す応答信号を生成する。パスワードの変更が書き換え可能であれば、応答信号「1」、ハードディスク障害などによりパスワードの書き換えが不可能であれば応答信号「0」を生成し、生成した応答信号を管理サーバ600へ送信する。

管理サーバは、第1アプリサーバ200aから応答信号を受信し、受信した応答信号が「1」であれば、第2アプリサーバ200bにも同様にユーザIDと暗号化現パスワードと暗号化新パスワードとを送信し、パスワード変更が可能か否かを問い合わせ、応答信号「1」を受信すると、次のアプリサーバ200へ、同様の問合せを行う。

全てのアプリサーバ200から、応答信号「1」を受信すると、管理サーバ600は、全てのアプリサーバ200へ、パスワード変更を指示する。

各アプリサーバ200は管理サーバ600からパスワード変更の指示を受信し、前もって受信している暗号化現パスワードと暗号化新パスワードとを復号して、現パスワードと新パスワードとを生成し、受信したユーザIDと生成した現パスワードとを含むパスワード情報を選択し、選択したパスワード情報に含まれるパスワードを生成した新パスワードに書き換える。

次に、管理サーバ600は、ユーザ端末に端末用変更完了画面データを送信し、パスワードの変更が正常に終了したことを通知する。

パスワード変更が可能か否かの問合せの途中に、何れかのアプリサーバ200から応答信号「0」を受信すると、該当するアプリサーバ200のパスワード変更は不可能であると判断し、既にパスワード変更の問合せを行ったアプリサーバ200全てに、パスワード変更の中止を知らせる。

次に、ユーザ端末に端末用変更失敗画面データを送信し、パスワード変更が失敗したことを通知する。

(4) タイムアウトによる判断

また上記の(3)において、各アプリサーバ200にパスワード変更が可能か否かを問い合わせる際に、問合せを送信してからの時間を計測し、あらかじめ設定しておいた最大待ち時間を超えても応答信号を受信しないとき、該当するアプリサーバ200のパスワード変更は不可能であると判断するとしてもよい。

(5) 専用線による接続

実施の形態3において、パスワード変更システムは、パスワード変更用の専用線を備えるとしてもよい。

具体的には、管理サーバ600と各アプリサーバ200とは専用線で直接接続されている。通常のサービスの提供には、上記の実施の形態3において説明したように、バス33及び34を介して、情報の送受信を行う。

(6) アプリサーバ200の処理状況

上記の実施の形態1～3において、管理サーバ600は、各アプリサーバ200の処理状況を記憶しており、これに応じてパスワードの変更の実施を中止するとしてもよい。

具体的には、管理サーバ600は、ルーティングテーブル641に代わって、ルーティングテーブル641bを記憶している。

ルーティングテーブル641bは、図43に示すように、複数のルート情報642b、643b・・・から構成される。各ルート情報は、アプリ番号、ホスト名、IPアドレス、ポート番号及び処理状況から構成

される。アプリ番号、ホスト名、IPアドレス及びポート番号は、上記のルーティングテーブル641に含まれるアプリ番号、ホスト名、IPアドレス及びポート番号と同様であるので、説明を省略する。処理状況は、アプリ番号の示すアプリサーバ200の処理状況を示している。処理状況「通常」は、アプリ番号の示すアプリサーバ200が通常のサービス提供処理を行っていることを示す。処理状況「メンテナンス中」は、アプリ番号の示すアプリサーバ200がメンテナンス中であることを示しており、管理サーバ600は、処理状況「メンテナンス中」の場合、該当するアプリサーバ200のパスワード変更の処理ができないことを判別する。

管理サーバ600は、各アプリサーバ200に定期的に監視信号を送信する。

各アプリサーバ200は、管理サーバ600から監視信号を受信し、自身の処理状態が通常であれば応答信号「通常」を返信する。自身の処理状況がメンテナンス中であれば応答信号「メンテナンス」を返信する。

管理サーバ600は、各アプリサーバ200から応答信号を受信し、受信した応答状況を基に、記憶しているルーティングテーブル641bの各アプリサーバ200の処理状況を書き換える。

ユーザ端末又は内部ユーザ端末から、パスワード変更の要求を受信すると、管理サーバ600は、ルーティングテーブル641bの処理状況を確認し、全てのアプリサーバ200の処理状況が「通常」であると判断すると、上述したようなパスワード変更の処理を開始する。

処理状況が「通常」でないアプリサーバ200が1つでも存在すれば、ユーザ端末へ、現在パスワードの変更を受け付けられない旨を通知する。

また、管理サーバ600からの監視信号の有無にかかわらず、各アプリサーバ200が自発的に、管理サーバ600に自身の処理状況を報告するとしてもよい。

(7) アプリサーバによる現パスワードの記憶

実施の形態1～3において、管理サーバ600がパスワード変更テ

ブル 6 5 1 により、現パスワードと新パスワードとを記憶しているが、各アプリサーバ 2 0 0 が記憶しているとしてもよい。

この場合、管理サーバ 6 0 0 は、第 1 アプリサーバ 2 0 0 a から第 4 アプリサーバ 2 0 0 d の順に、ユーザ I D と暗号化現パスワードと暗号化新パスワードとを送信し、パスワード変更を指示する。

各アプリサーバ 2 0 0 は、ユーザ I D と暗号化現パスワードと暗号化新パスワードとを受信し、受信した暗号化現パスワードと暗号化新パスワードとを復号し、ユーザ I D と現パスワードとを含むパスワード情報を選択し、選択したパスワード情報に含まれるパスワードを新パスワードに書き換える。書き換えが成功すれば、終了信号「1」を管理サーバへ送信する。次に、書き換えたパスワード情報に対応付けて、現パスワードを記憶しておく。

管理サーバ 6 0 0 は、アプリサーバ 2 0 0 から終了信号の受信し、受信した終了信号が「1」であれば、次のアプリサーバ 2 0 0 へユーザ I D と暗号化現パスワードと暗号化新パスワードとを送信する。

受信した終了信号が「0」である場合、又は一定時間を超えて終了信号を受信しない場合、パスワードの変更が失敗であると判断し、既に終了信号「1」を受信済みのアプリサーバ 2 0 0 に、パスワード復旧の指示を送信する。

パスワード復旧の指示を受信したアプリサーバ 2 0 0 は、書き換えたパスワード情報のパスワードを、記憶している現パスワードに書き換える。

(8) 初期パスワードへの変更

実施の形態 1 ～ 3 において、利用者がパスワードを忘れている場合、パスワードを初期パスワードに変更するとしてもよい。

初期パスワードとは、パスワード変更システムの管理者側から利用者に最初に割り当てられるパスワードであり、メール、書面などで利用者に通達されるものである。一例として「0 0 0 0」のような簡単な文字列やユーザ I D と同じ文字列が挙げられる。

具体的には、管理サーバ600は、あらかじめ各利用者の初期パスワードを記憶している。

ログイン画面151に、さらに、パスワード忘れボタンを設けておき、利用者は、パスワードを忘れた場合にパスワード忘れボタンを選択する。

5 ユーザ端末は、パスワード忘れボタンの押下を検出すると、管理サーバ600へパスワード忘れを通知する。

管理サーバ600は、ユーザ端末からパスワード忘れの通知を受信すると、叙述したようなパスワード変更の処理を開始する。このとき、利用者により入力された新パスワードに代わって初期パスワードを各アプリサーバ200へ送信し、パスワードの変更を指示する。

10 全てのアプリサーバ200のパスワード変更が成功すると、ユーザ端末へパスワードを初期パスワードに変更したことを通知する。

産業上の利用の可能性

15 本発明の各装置及びシステムは、各種のサービスをネットワークを介して、利用者に提供する産業において、経営的に、また継続的及び反復的に使用することができる。また、本発明を構成する各装置、コンピュータプログラム及び記録媒体は、電器機器製造産業において、経営的に、また継続的及び反復的に、製造し、販売することができる。

20

25

請 求 の 範 囲

1. 一のパスワードにより認証した一の利用者へ各サービスを提供する複数のアプリケーション装置に対して、当該パスワードの更新を指示する管理サーバ装置であって、

全てのアプリケーション装置のパスワードの更新を試みる第1手段と、各アプリケーション装置について、パスワードの更新が不可能か否かを判断する第2手段と、

不可能と判断されるアプリケーション装置が少なくとも1台存在する場合に、全てのアプリケーション装置のパスワードを更新前のものとする第3手段と

を備えることを特徴とする管理サーバ装置。

2. 前記管理サーバ装置は、さらに、

利用者装置からパスワードの更新の要求を受信する第4手段を含み、前記第1手段は、受信した前記更新の要求に基づいて、パスワードの更新を試みる

ことを特徴とする請求の範囲1に記載の管理サーバ装置。

3. 前記第1手段は、全てのアプリケーション装置に対してパスワードの更新を指示し、

前記第2手段は、各アプリケーション装置について、パスワードの更新が失敗したか否かを判断し、

前記第3手段は、少なくとも1台のアプリケーション装置について、更新が失敗したと判断される場合に、パスワードの更新が成功した他のアプリケーション装置に対して、更新前のパスワードへの復元を指示する

ことを特徴とする請求の範囲2に記載の管理サーバ装置。

4. 前記第4手段は、利用者の新パスワードと旧パスワードとを含む前記更新の要求を受信し、

前記第1手段は、受信した更新の要求に含まれる新パスワードと旧パ

スワードとを含む更新の指示を生成し、生成した前記更新の指示を全てのアプリケーション装置に対して送信する

ことを特徴とする請求の範囲 3 に記載の管理サーバ装置。

5. 前記第 2 手段は、

- 5 各アプリケーション装置からのパスワードの更新の成功又は失敗を示す応答を受信する応答受信部と、

受信した前記応答が成功を示す場合に、当該アプリケーション装置についてパスワードの更新が成功したと断定し、受信した前記応答が失敗を示す場合に、当該アプリケーション装置についてパスワードの更新が

- 10 失敗したと断定する断定部と

を含むことを特徴とする請求の範囲 3 に記載の管理サーバ装置。

6. 前記第 2 手段は、

時間の経過に伴って経過時間を計測する計時部と、

- 15 前記第 1 手段による更新の指示の送信の時点において、計時部により計測される経過時間を初期値にリセットする初期化部と、

各アプリケーション装置からのパスワードの更新の成功又は失敗を示す応答を待ち受ける待受部と、

計測された経過時間が、所定のしきい値より大きいか否かを判断する判断部と、

- 20 判断部により経過時間が前記しきい値と等しいか又は小さいと判断され、かつ待受部により各アプリケーション装置からの応答を受信し、かつその応答が成功を示す場合に、当該アプリケーション装置について、パスワードの更新が成功したと断定し、その他の場合に、当該アプリケーション装置について、パスワードの更新が失敗したと断定する断定部と
- 25

を含むことを特徴とする請求の範囲 3 に記載の管理サーバ装置。

7. 前記第 1 手段は、全てのアプリケーション装置に対してパスワードの更新の準備を指示し、

前記第 2 手段は、各アプリケーション装置について、パスワードの更

新の準備が未完了か否かを判断し、

前記第3手段は、少なくとも1台のアプリケーション装置について、更新の準備が未完了と判断される場合に、更新の準備が完了した他のアプリケーション装置に対して、前記更新の準備の指示を取り消す

5 ことを特徴とする請求の範囲2に記載の管理サーバ装置。

8. 前記第4手段は、利用者の新パスワードと旧パスワードとを含む前記更新の要求を受信し、

前記第1手段は、受信した更新の要求に含まれる新パスワードと旧パスワードとを含む更新の準備の指示を生成し、生成した前記更新の準備
10 の指示を全てのアプリケーション装置に対して送信する

ことを特徴とする請求の範囲7に記載の管理サーバ装置。

9. 前記第2手段は、

アプリケーション装置からのパスワードの更新の準備の完了又は未完了を示す応答を受信する応答受信部と、

15 受信した前記応答が完了を示す場合に、当該アプリケーション装置についてパスワードの更新の準備が完了したと断定し、受信した前記応答が未完了を示す場合に、当該アプリケーション装置についてパスワードの更新の準備が未完了であると断定する断定部と

を含むことを特徴とする請求の範囲7に記載の管理サーバ装置。

20 10. 前記第2手段は、

時間の経過に伴って経過時間を計測する計時部と、

前記第1手段による更新の準備の指示の送信の時点において、計時部により計測される経過時間を初期値にリセットする初期化部と、

アプリケーション装置からのパスワードの更新の準備の完了又は未完了を示す応答を待ち受ける待受部と、
25

計測された経過時間が、所定のしきい値より大きいか否かを判断する判断部と、

、判断部により経過時間が前記しきい値と等しいか又は小さいと判断され、かつ待受部によりアプリケーション装置からの応答を受信し、かつ

その応答が完了を示す場合に、パスワードの更新の準備が完了したと断定し、その他の場合に、パスワードの更新の準備が未完了であると断定する断定部と

を含むことを特徴とする請求の範囲 7 に記載の管理サーバ装置。

5 1 1. 前記管理サーバ装置は、さらに、

前記第 2 手段によりパスワードの更新が不可能と判断される場合に、元のパスワードに戻す旨のメッセージを前記利用者装置へ送信するメッセージ送信手段

を含むことを特徴とする請求の範囲 2 に記載の管理サーバ装置。

10 1 2. 前記管理サーバ装置は、さらに、

各アプリケーション装置について、メンテナンス中であるか否かを記憶している管理記憶手段を備え、

前記第 1 手段は、メンテナンス中のアプリケーション装置が存在しない場合に、パスワードの更新を試みる

15 ことを特徴とする請求の範囲 2 に記載の管理サーバ装置。

1 3. 前記第 1 手段は、メンテナンス中のアプリケーション装置が存在する場合に、パスワードの更新を中止し、

前記管理サーバ装置は、さらに、

20 前記第 1 手段によりパスワードの更新が中止される場合に、パスワードの更新を中止する旨のメッセージを前記利用者装置へ送信するメッセージ送信手段を含む

ことを特徴とする請求の範囲 2 に記載の管理サーバ装置。

1 4. 前記アプリケーション装置は、第 1 ネットワークを介して、前記管理サーバ装置と接続されており、

25 前記利用者装置は、第 1 ネットワークに接続されていない第 2 ネットワークを介して、前記管理サーバ装置と接続されている

ことを特徴とする請求の範囲 2 に記載の管理サーバ装置。

1 5. 前記第 1 ネットワーク及び前記第 2 ネットワークは、イントラネットである

ことを特徴とする請求の範囲 1 4 に記載の管理サーバ装置。

1 6. 前記管理サーバ装置と、各アプリケーション装置とは、専用線を介して、接続されており、

5 パスワードの更新の際には、前記管理サーバ装置は、前記専用線を介して、各アプリケーション装置との間で、パスワードの更新のための情報を送受信し、

各サービスの提供の際には、前記管理サーバ装置は、第 1 及び第 2 ネットワークを介して、前記利用者装置と各アプリケーション装置との間で、前記サービスに係る情報の送受信を中継する

10 ことを特徴とする請求の範囲 1 4 に記載の管理サーバ装置。

1 7. 前記アプリケーション装置及び前記利用者装置は、ネットワークを介して、前記管理サーバ装置と接続されており、

前記管理サーバ装置は、さらに、

15 アプリケーションの種類と、各アプリケーション装置のネットワーク上における位置情報とを対応付ける対応テーブルを記憶している記憶手段と、

前記利用者装置から、アプリケーションを示す種類情報と処理の内容を示す処理情報とを受信する受信手段と、

20 前記対応テーブルを用いて、受信した種類情報に対応するアプリケーション装置の位置情報を取得する取得手段と、

取得した位置情報により示されるアプリケーション装置に対して、前記処理情報を送信する送信手段と

を含むことを特徴とする請求の範囲 2 に記載の管理サーバ装置。

1 8. 前記ネットワークは、インターネットである

25 ことを特徴とする請求の範囲 1 6 に記載の管理サーバ装置。

1 9. 更新後の新パスワードは、利用者に最初に割り当てられた初期パスワードであり、

前記第 1 手段は、全てのアプリケーション装置の初期パスワードへの更新を試み、

前記第 2 手段は、各アプリケーション装置について、初期パスワードへの更新が不可能か否かを判断し、

- 前記第 3 手段は、不可能と判断されるアプリケーション装置が少なくとも 1 台存在する場合に、全てのアプリケーション装置のパスワードを
5 更新前のものとする

ことを特徴とする請求の範囲 1 に記載の管理サーバ装置。

20. 一のパスワードにより認証した一の利用者へサービスを提供し、管理サーバ装置からの指示によりパスワードを更新するアプリケーション装置であって、

- 10 更新前のパスワードを記憶している旧パスワード記憶手段と、
利用者の認証に用いるパスワードを記憶している認証用パスワード記憶手段と、

管理サーバ装置から、パスワードを更新前のものに復元する復元指示を受信する受信手段と、

- 15 前記復元指示を受信すると、旧パスワード記憶手段から更新前のパスワードを読み出し、読み出したパスワードを認証用パスワード記憶手段に上書きする書込手段と

を備えることを特徴とするアプリケーション装置。

- 20 21. 前記アプリケーション装置は、前記管理サーバ装置を介して、利用者の利用者装置との間で、前記サービスに関する情報の送受信を行う

ことを特徴とする請求の範囲 20 に記載のアプリケーション装置。

22. 前記アプリケーション装置は、メンテナンス中である場合に、当該旨を前記管理サーバ装置に対して通知する

ことを特徴とする請求の範囲 21 に記載のアプリケーション装置。

- 25 23. 前記アプリケーション装置は、第 1 ネットワークを介して、前記管理サーバ装置と接続されており、

前記利用者装置は、第 1 ネットワークに接続されていない第 2 ネットワークを介して、前記管理サーバ装置と接続されている

ことを特徴とする請求の範囲 21 に記載のアプリケーション装置。

24. 前記アプリケーション装置及び前記管理サーバ装置は、専用線を介して接続されており、

パスワードの更新の際には、前記管理サーバ装置は、前記専用線を介して、前記管理サーバとの間で、パスワードの更新のための情報を送受信し、

各サービスの提供の際には、第1及び第2ネットワークを介して、前記サービスに係る情報を送受信する

ことを特徴とする請求の範囲23に記載のアプリケーション装置。

25. 前記アプリケーション装置及び前記利用者装置は、インターネットを介して、前記管理サーバ装置と接続されている

ことを特徴とする請求の範囲21に記載のアプリケーション装置。

26. 利用者の端末装置と、一のパスワードにより認証した一の利用者の端末装置へ各サービスを提供する複数のアプリケーション装置と、前記アプリケーション装置に対して、当該パスワードの更新を指示する管理サーバ装置とから構成されるパスワード更新システムであって、

前記管理サーバ装置は、

全てのアプリケーション装置のパスワードの更新を試みる第1手段と、各アプリケーション装置について、パスワードの更新が不可能か否かを判断する第2手段と、

不可能と判断されるアプリケーション装置が少なくとも1台存在する場合に、全てのアプリケーション装置のパスワードを更新前のものとする第3手段とを備え、

各アプリケーション装置は、

更新前のパスワードを記憶している旧パスワード記憶手段と、

25 利用者の認証に用いるパスワードを記憶している認証用パスワード記憶手段と、

管理サーバ装置から、パスワードを更新前のものに復元する復元指示を受信する受信手段と、

前記復元指示を受信すると、旧パスワード記憶手段から更新前のパス

ワードを読み出し、読み出したパスワードを認証用パスワード記憶手段に上書きする書込手段とを備える

ことを特徴とするパスワード更新システム。

27. 前記端末装置と各アプリケーション装置とは、前記管理サーバ装置を介して、情報の送受信を行う

ことを特徴とする請求の範囲26に記載のパスワード更新システム。

28. 前記アプリケーション装置は、第1ネットワークを介して、前記管理サーバ装置と接続されており、

10 前記利用者装置は、第1ネットワークに接続されていない第2ネットワークを介して、前記管理サーバ装置と接続されている

ことを特徴とする請求の範囲27に記載のパスワード更新システム。

29. 前記第1ネットワーク及び前記第2ネットワークは、イントラネットである

ことを特徴とする請求の範囲28に記載のパスワード更新システム。

15 30. 前記管理サーバ装置と、各アプリケーション装置とは、専用回線を介して、接続されており、

パスワードの更新の際には、前記管理サーバ装置は、前記専用線を介して、前記管理サーバとの間で、パスワードの更新のための情報を送受信し、

20 各サービスの提供の際には、第1及び第2ネットワークを介して、前記サービスに係る情報を送受信する

ことを特徴とする請求の範囲28に記載のパスワード更新システム。

31. 前記アプリケーション装置及び前記利用者装置は、ネットワークを介して、前記管理サーバ装置と接続されており、

25 前記管理サーバ装置は、さらに、

アプリケーションの種類と、各アプリケーション装置のネットワーク上における位置情報とを対応付ける対応テーブルを記憶している記憶手段と、

前記利用者装置から、アプリケーションを示す種類情報と処理の内容

を示す処理情報とを受信する受信手段と、

前記対応テーブルを用いて、受信した種類情報に対応するアプリケーション装置の位置情報を取得する取得手段と、

- 取得した位置情報により示されるアプリケーション装置に対して、前
5 記処理情報を送信する送信手段と

を含むことを特徴とする請求の範囲 27 に記載のパスワード更新システム。

32. 前記ネットワークは、インターネットである

ことを特徴とする請求の範囲 30 に記載のパスワード更新システム。

- 10 33. 一のパスワードにより認証した一の利用者へ各サービスを提供する複数のアプリケーション装置に対して、当該パスワードの更新を指示する管理サーバ装置で用いられる管理サーバ制御方法であって、

全てのアプリケーション装置のパスワードの更新を試みる第 1 ステップと、

- 15 各アプリケーション装置について、パスワードの更新が不可能か否かを判断する第 2 ステップと、

不可能と判断されるアプリケーション装置が少なくとも 1 台存在する場合に、全てのアプリケーション装置のパスワードを更新前のものとする第 3 ステップと

- 20 を含むことを特徴とする管理サーバ制御方法。

34. 一のパスワードにより認証した一の利用者へ各サービスを提供する複数のアプリケーション装置に対して、当該パスワードの更新を指示する管理サーバ装置で用いられる管理サーバ制御プログラムであって、

- 25 全てのアプリケーション装置のパスワードの更新を試みる第 1 ステップと、

各アプリケーション装置について、パスワードの更新が不可能か否かを判断する第 2 ステップと、

不可能と判断されるアプリケーション装置が少なくとも 1 台存在する場合に、全てのアプリケーション装置のパスワードを更新前のものとする

る第 3 ステップと

を含むことを特徴とする管理サーバ制御プログラム。

35. 前記管理サーバ制御プログラムは、

コンピュータ読み取り可能なプログラム記録媒体に記録されている

5 ことを特徴とする請求の範囲 34 に記載の管理サーバ制御プログラム。

10

15

20

25

図1

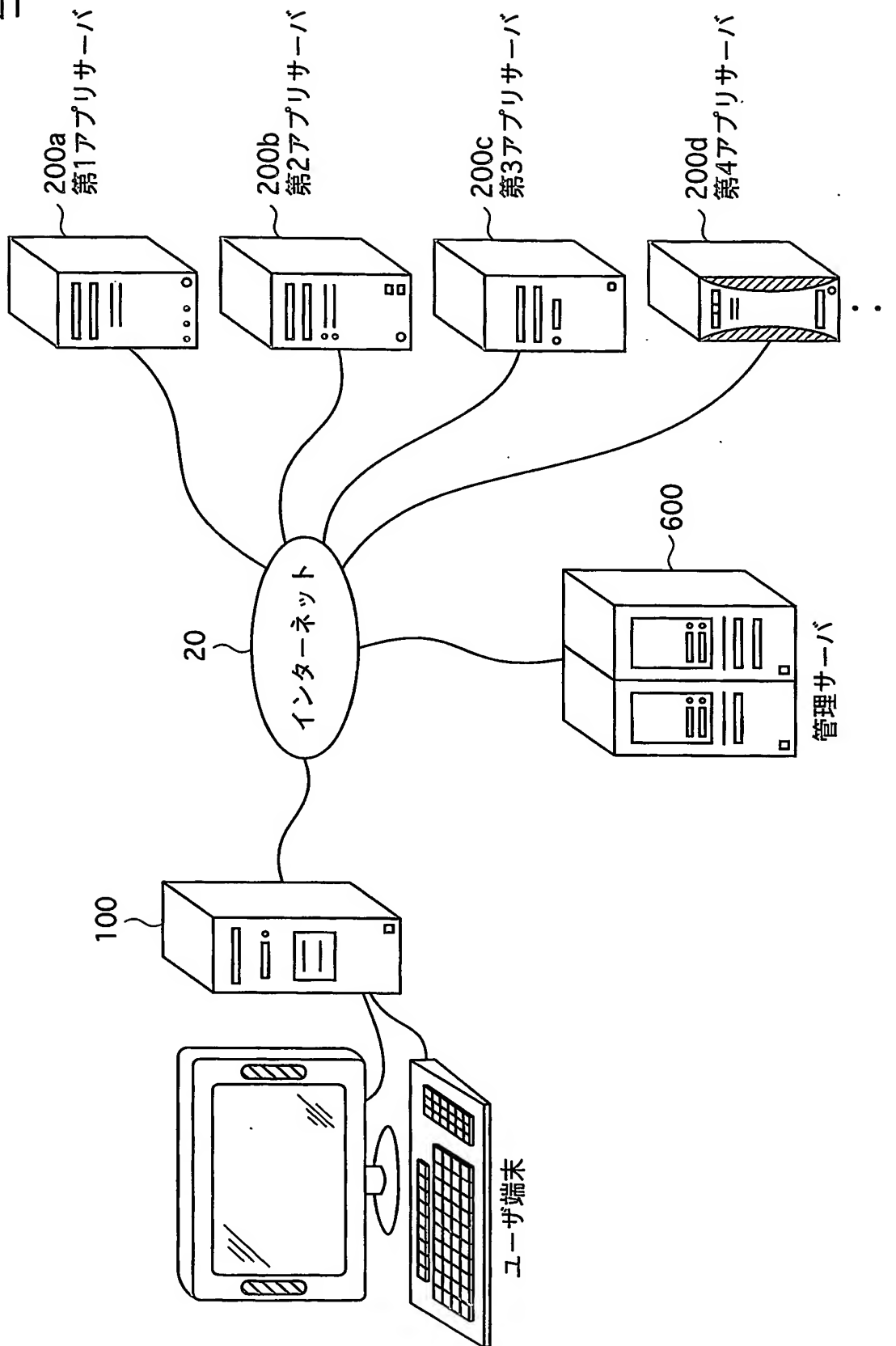


図2

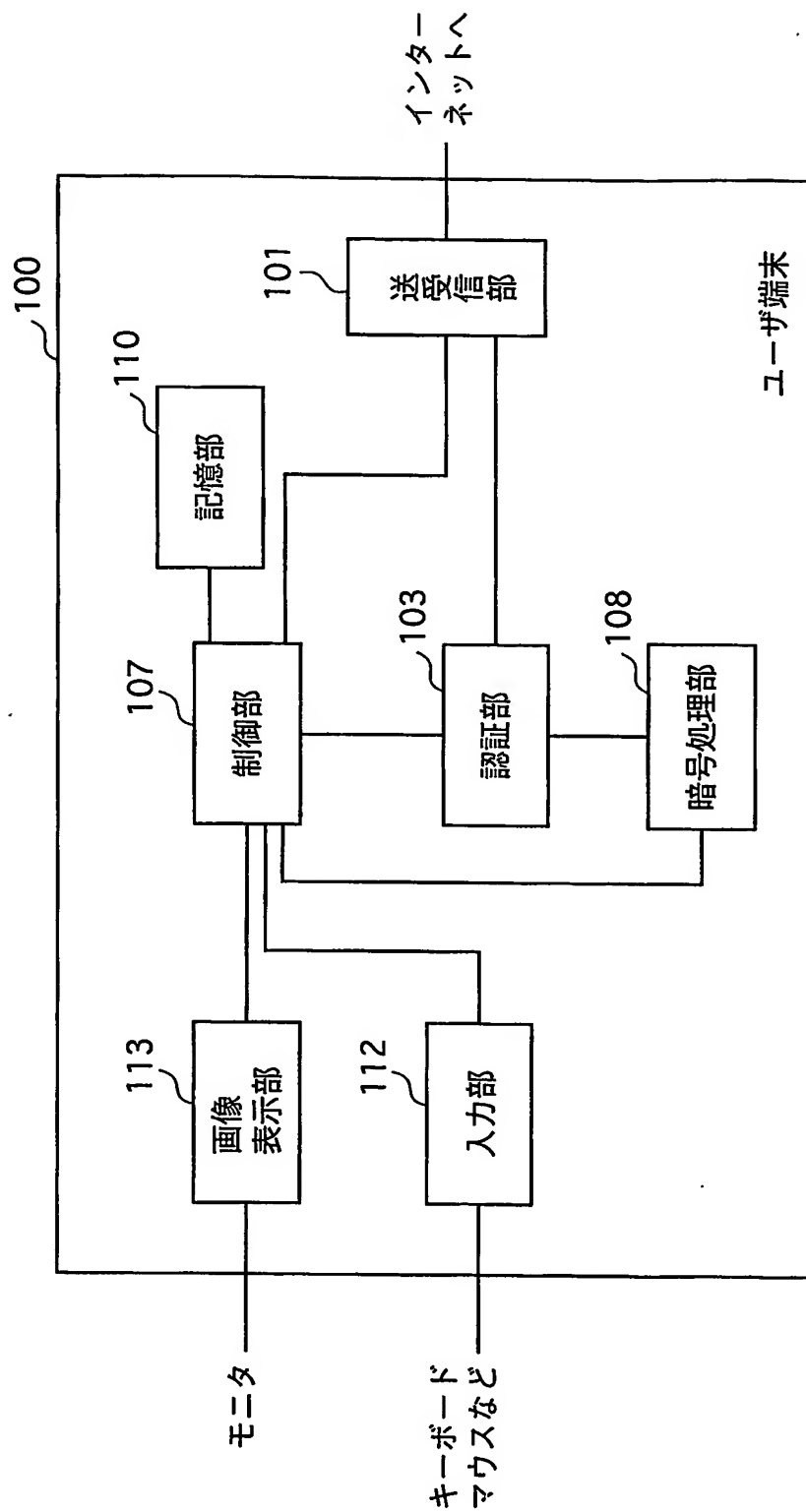


図3

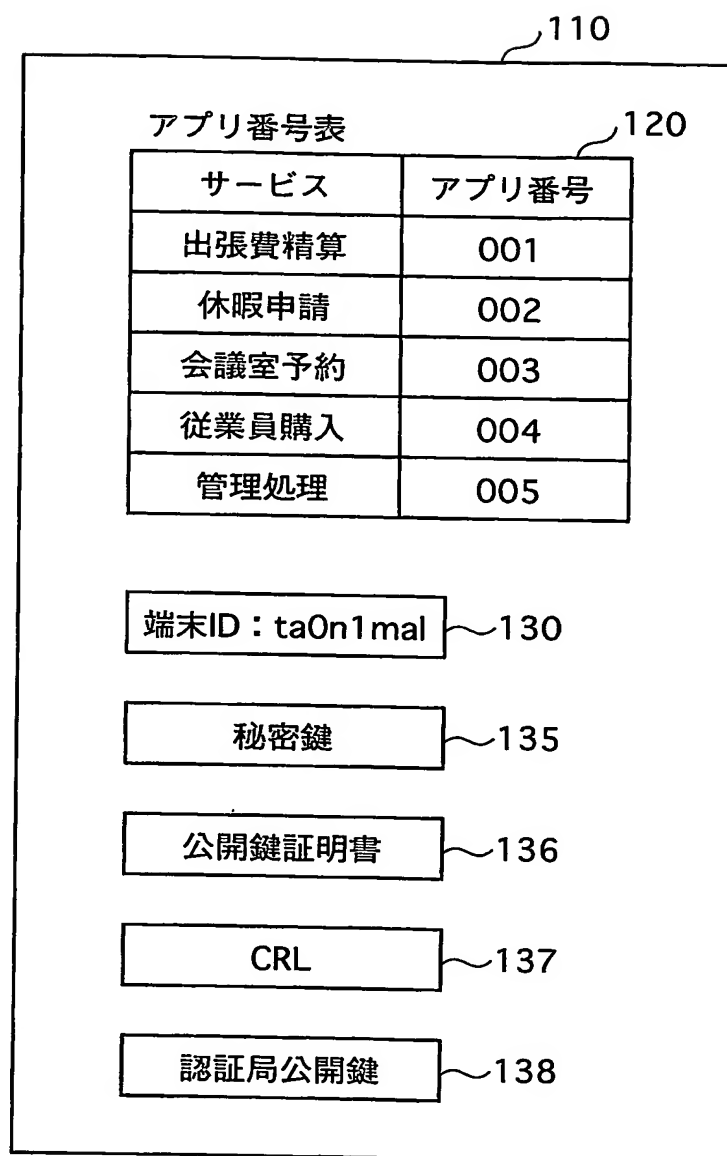
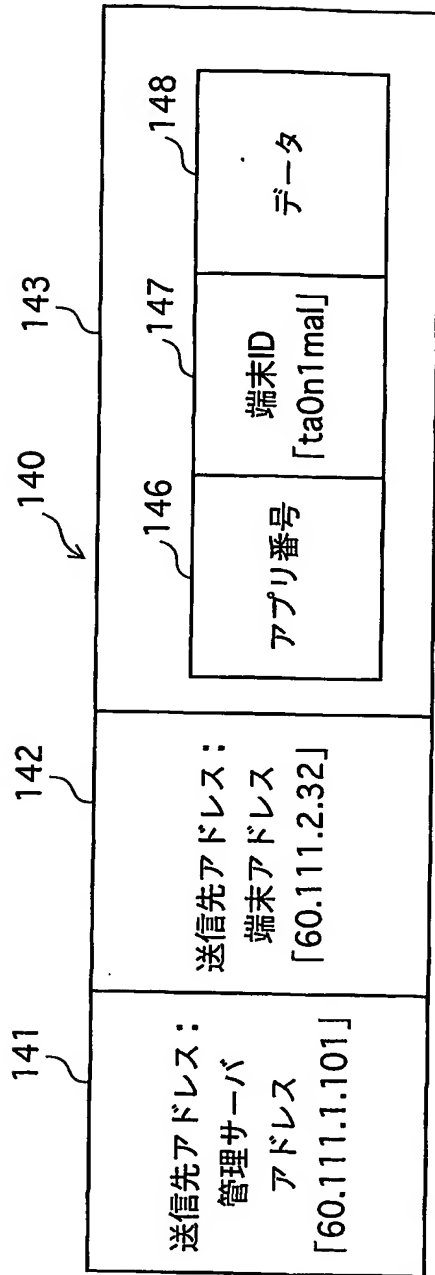


図4



データ 149

△△△××社			
2004.3.11			
地下鉄	〇〇駅発	△△駅着	××円
バス	〇〇駅発	××駅着	××円
△△△円			

図5

ログイン画面

151

ユーザID 152

パスワード 153

154

送信

メニュー画面

161

ユーザID maeda 氏名 前田博子

アプリケーション

出張費の精算 162

休暇申請 163

会議室予約 164

従業員購入 165

管理メニュー

パスワード変更 166

図6

精算画面

ユーザID maeda 氏名 前田博子

●必要事項を入力し、送信ボタンを押して下さい

出張先

出張日 年 月 日

交通機関		費用
<input type="text"/>	: <input type="text"/> 発 <input type="text"/> 着	: <input type="text"/> :
<input type="text"/>	: <input type="text"/> 発 <input type="text"/> 着	: <input type="text"/> :
<input type="text"/>	: <input type="text"/> 発 <input type="text"/> 着	: <input type="text"/> :

合計

173

171

精算終了画面

ユーザID maeda 氏名 前田博子

精算処理を正常に終了しました。

182

183

181

図7

パスワード変更画面

ユーザID maeda 氏名 前田博子

すべての空欄に記入し、送信ボタンを押して下さい

現在のパスワード 192

新しいパスワード 193

新しいパスワードをもう一度記入して下さい。

194

196

191

変更完了画面

ユーザID maeda 氏名 前田博子

パスワードの変更が正常に完了しました。

302 303

301

図8

変更失敗画面

ユーザID maeda 氏名 前田博子

パスワードの変更に失敗しました。
パスワードは変更前のままです。

メニューへ

ログアウト

311

強制終了画面

ユーザID maeda 氏名 前田博子

システムにエラーが発生しています。
強制終了します。

321

図9

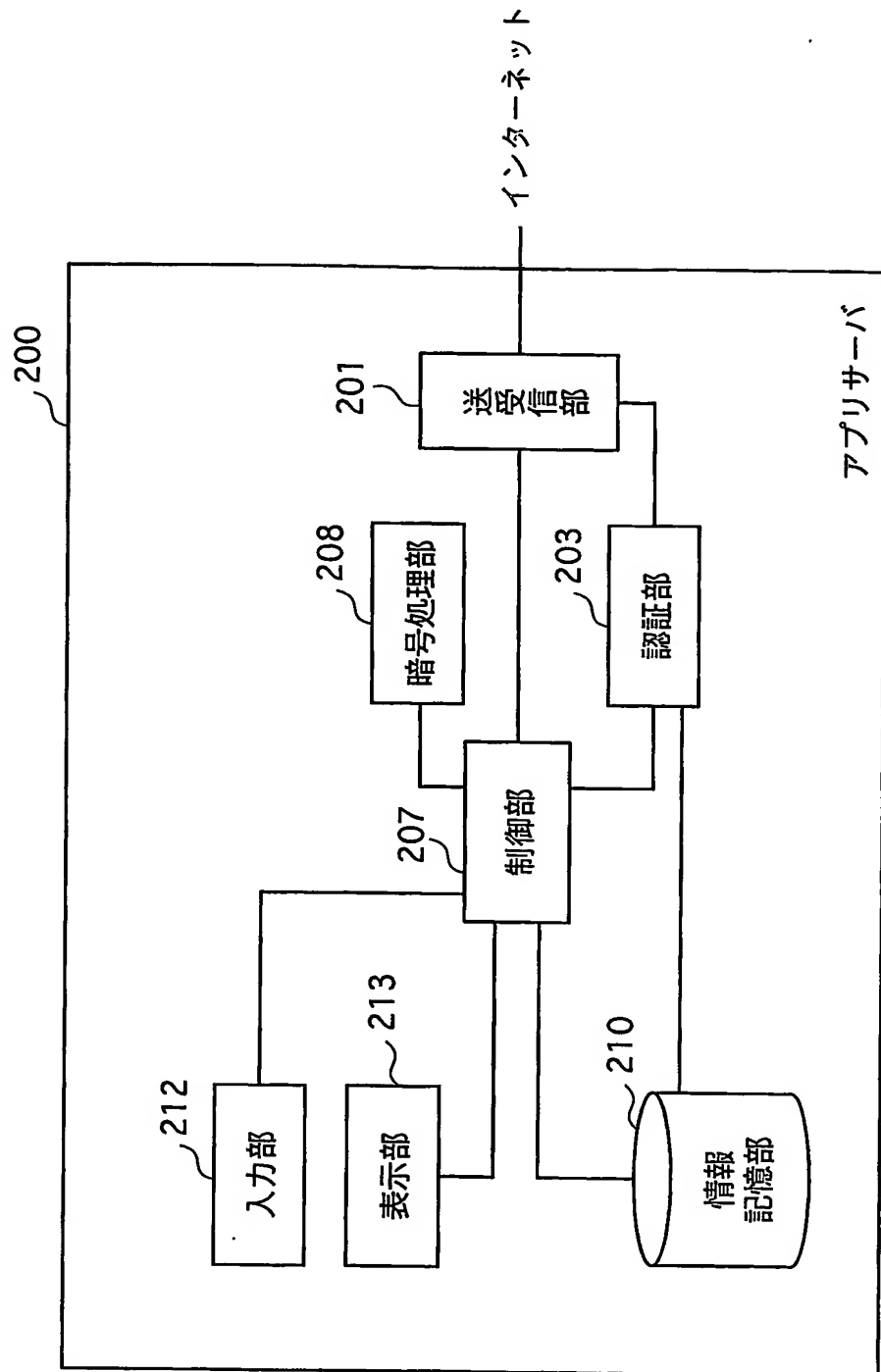


図10

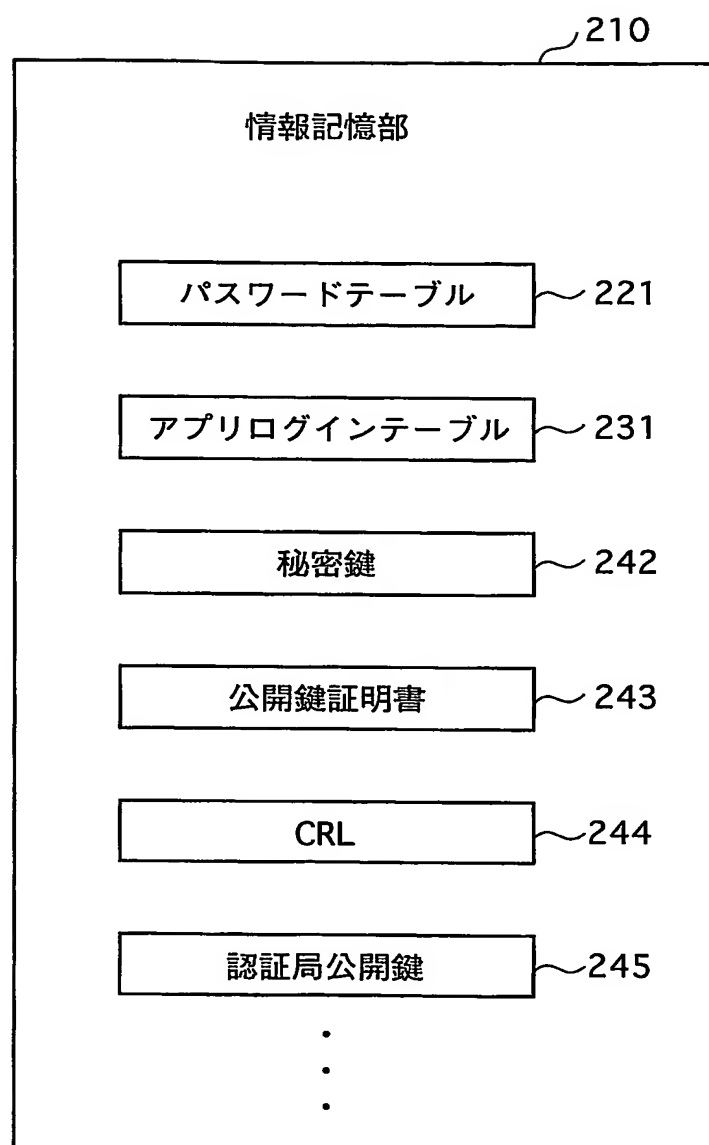


図11

パスワードテーブル

221

ユーザID	氏名	パスワード
223 ~ maeda	前田博子	ozy12
224 ~ nakamura	中村純一	klmoj
225 ~ suzuki	鈴木由香	spr01
・ ・ ・	・ ・ ・	・ ・ ・

図12

アプリログインテーブル

231

ユーザID	氏名	パスワード	端末ID
232 ~ maeda	前田博子	ozy12	ta0n1mal
233 ~ inoue	井上 宏	zz445	tzn1pps
・	・	・	・
・	・	・	・
・	・	・	・

図13

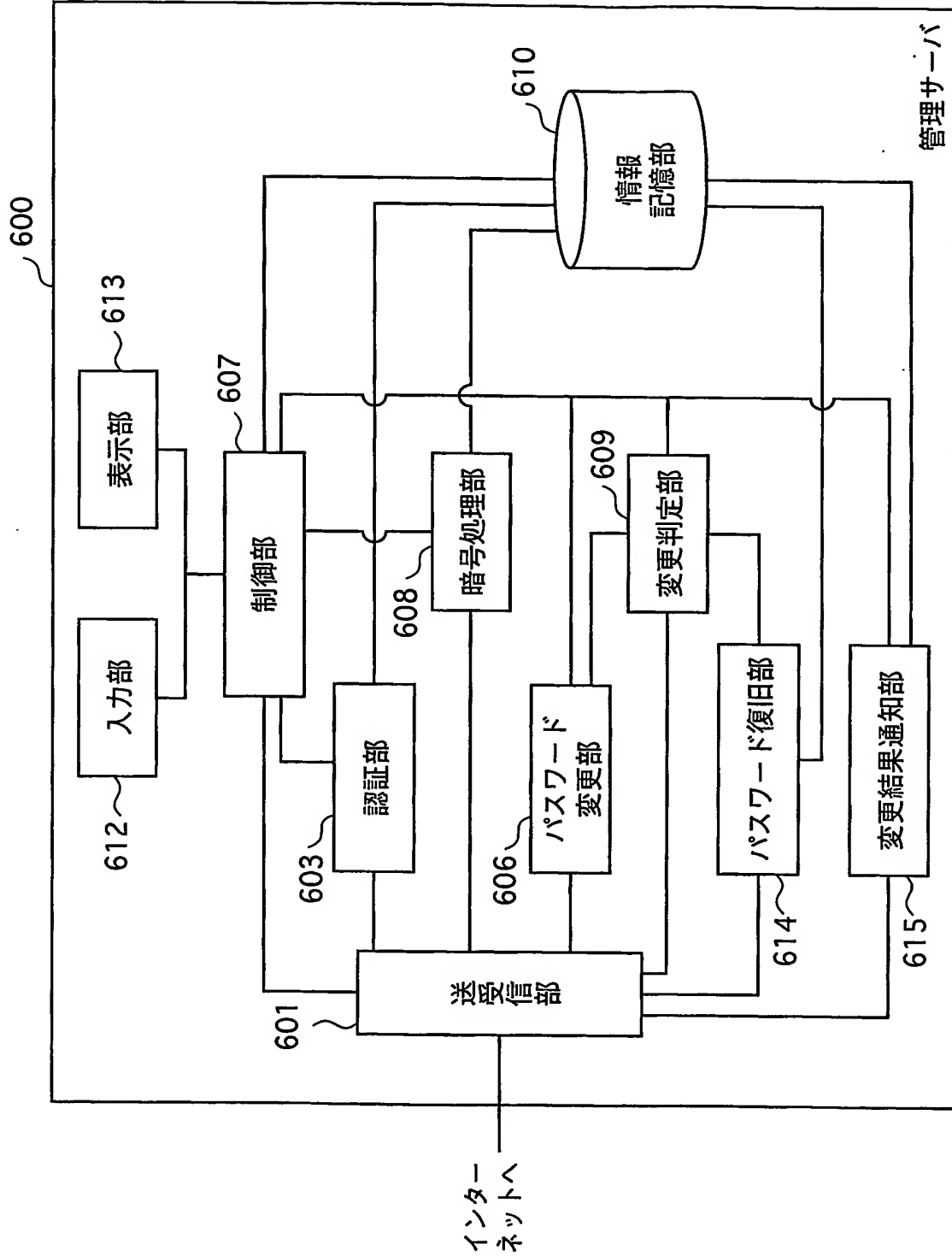


図14

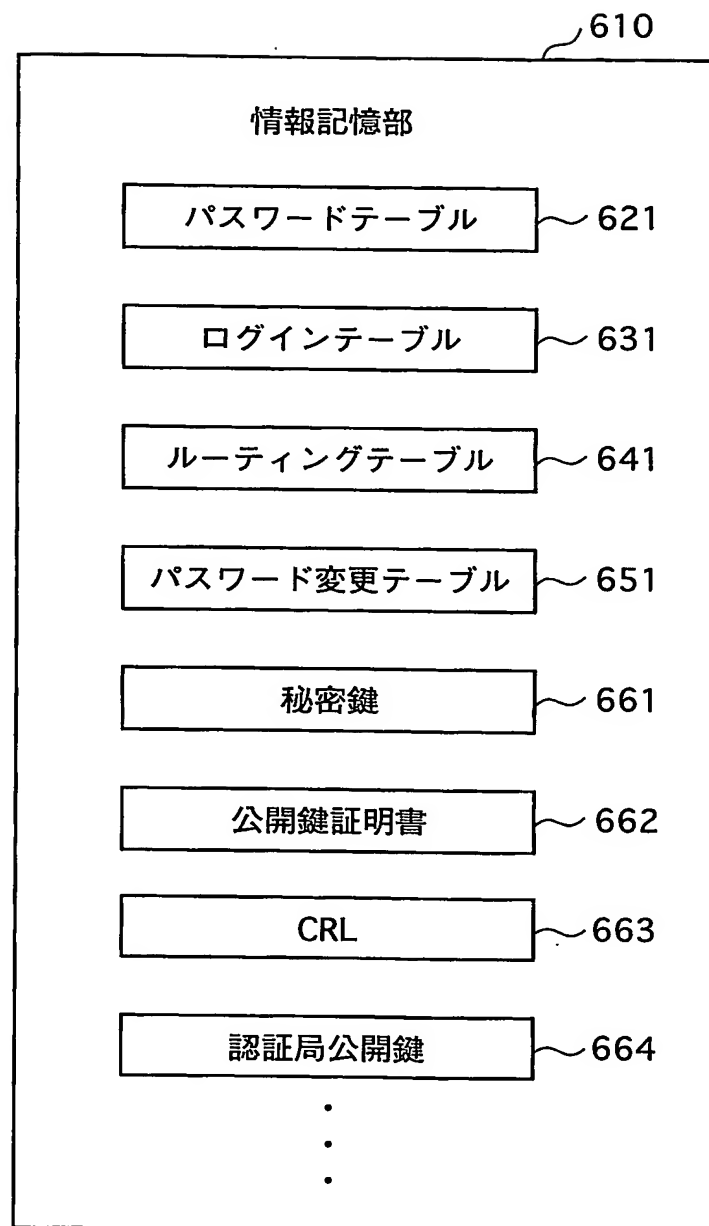


図15

ログインテーブル

631

ユーザID	氏名	パスワード	端末ID	処理状況
maeda	前田	ozy12	ta0n1mal	パスワード変更中
suzuki	鈴木	spr01	tz00mni	通常
inoue	井上	zz445	tn1pps	通常
.
.

632 ~

633 ~

634 ~

図16

ルーティングテーブル

641

アプリ番号	ホスト名	IPアドレス	ポート番号
642 ~ 001	system1	60.111.1.15	8000
643 ~ 002	system2	60.111.1.20	8001
⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮

図17

			651
	ユーザID	現パスワード	新パスワード
652	maeda	ozy12	nwy56
653	nakamura	klmOj	42try
654	suzuki	spr01	iksu7
⋮	⋮	⋮	⋮
	inoue	zz445	jty53

図18

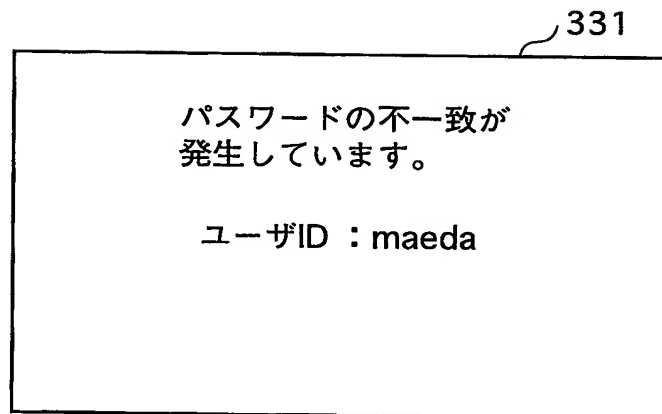


図19

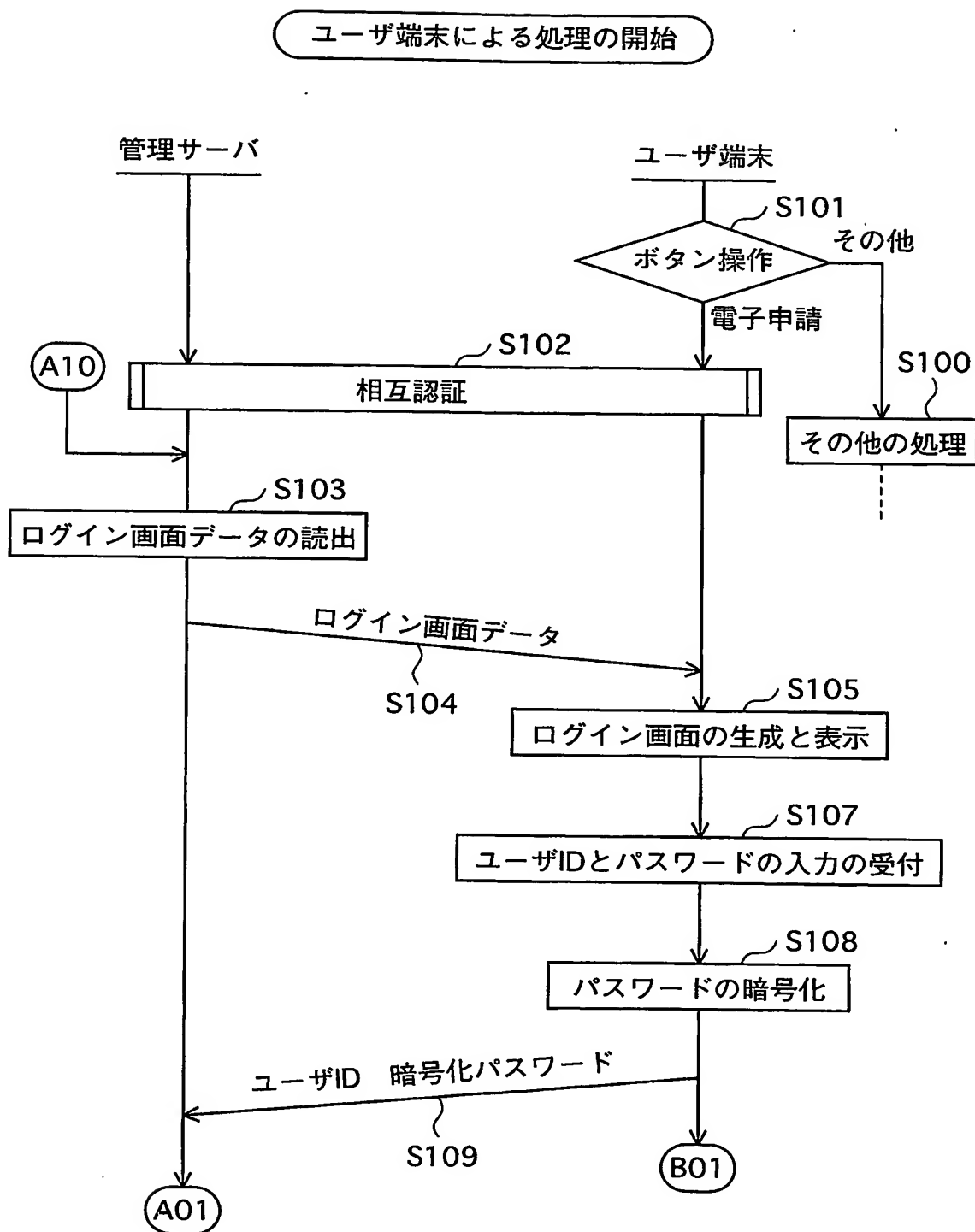


図20

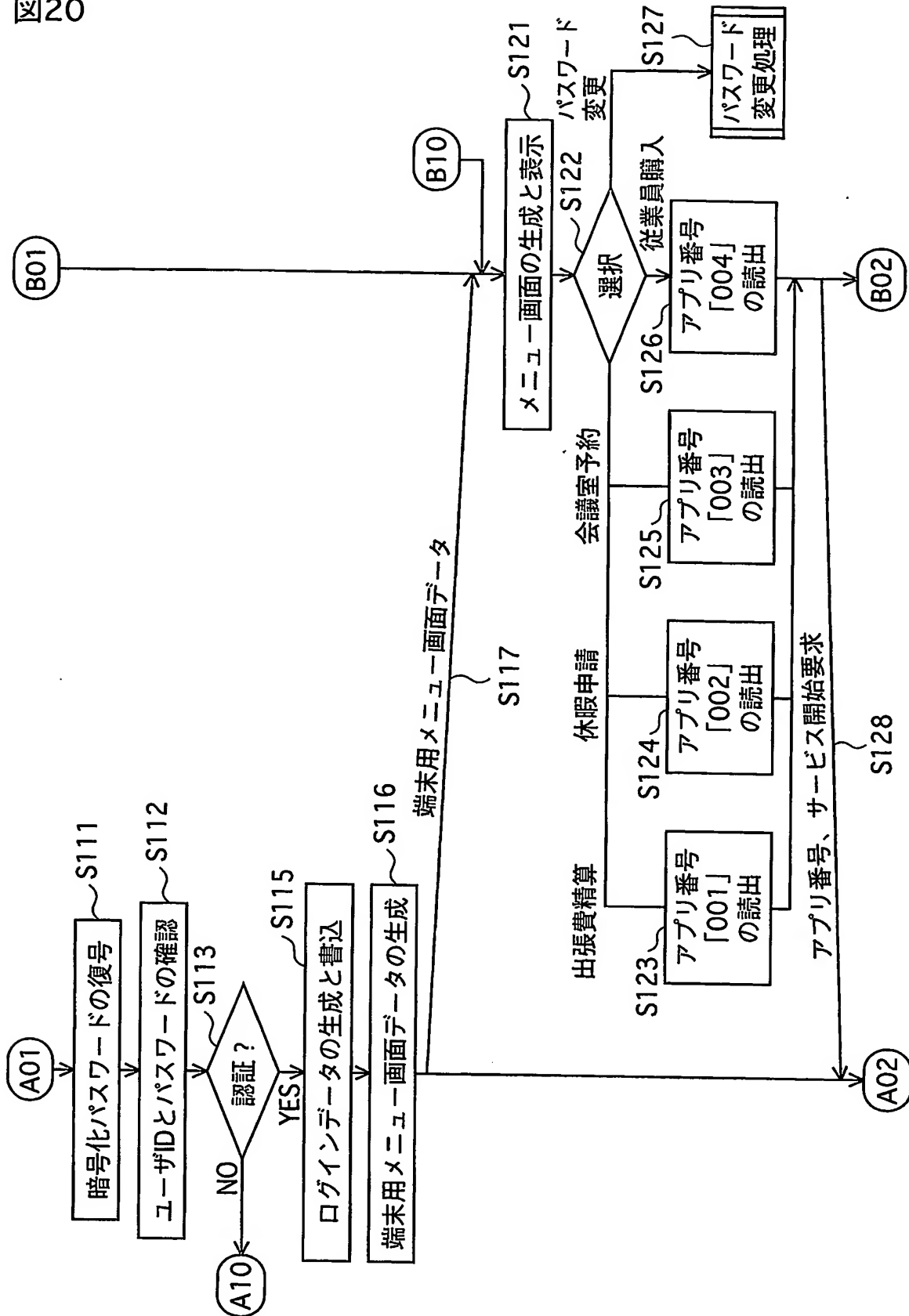


図21

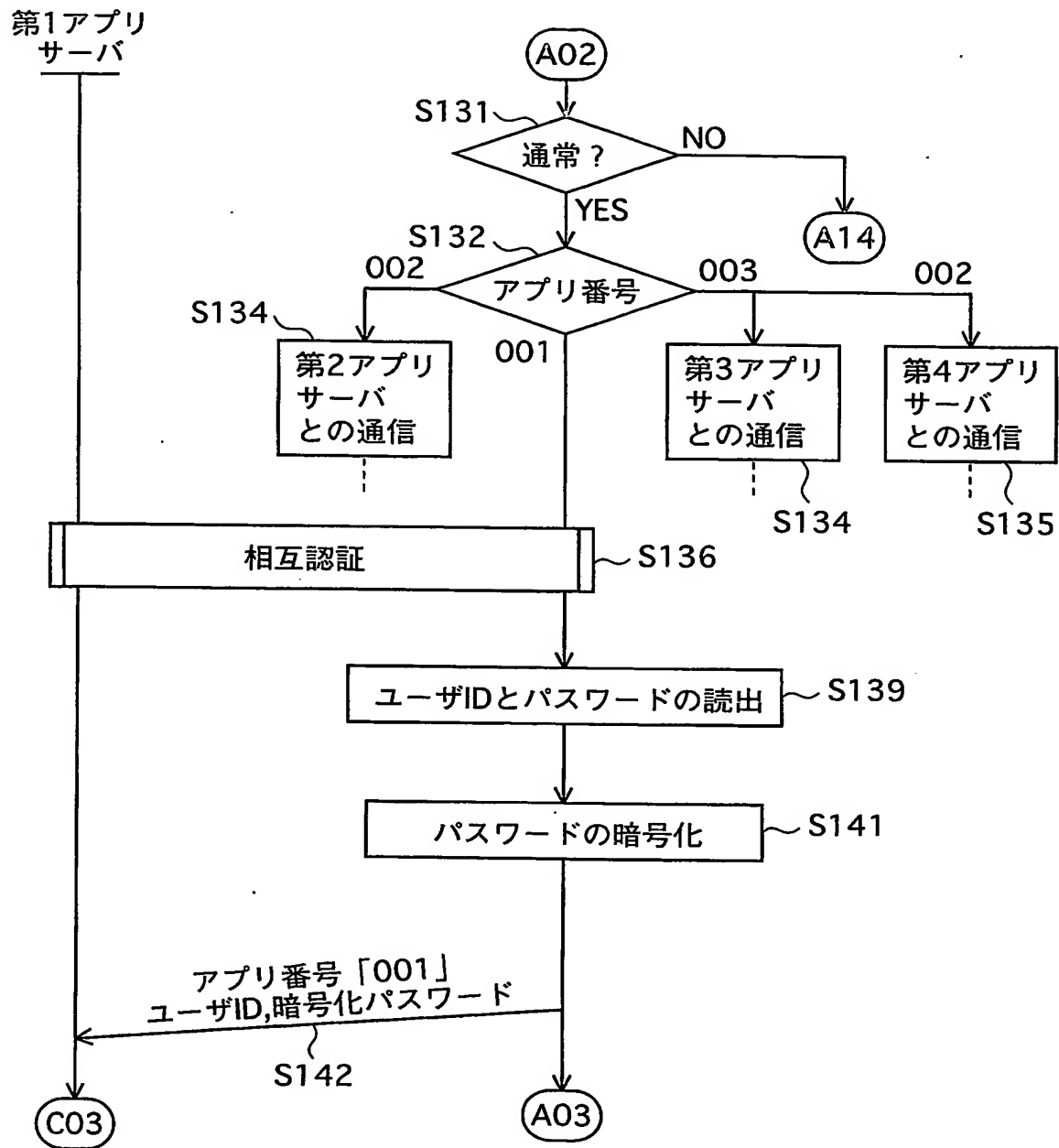


図22

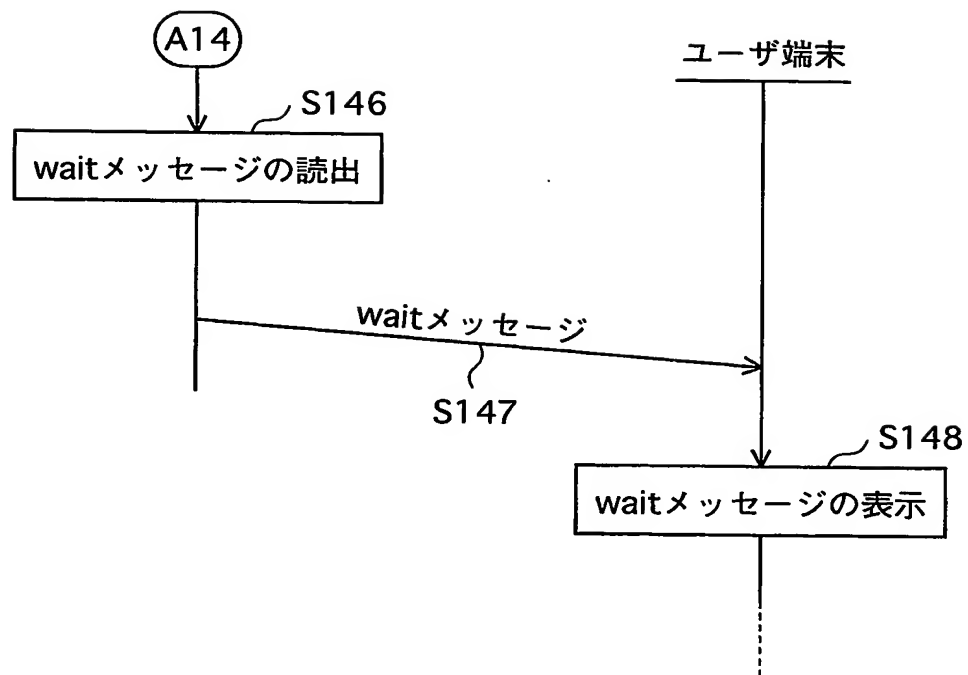


図23

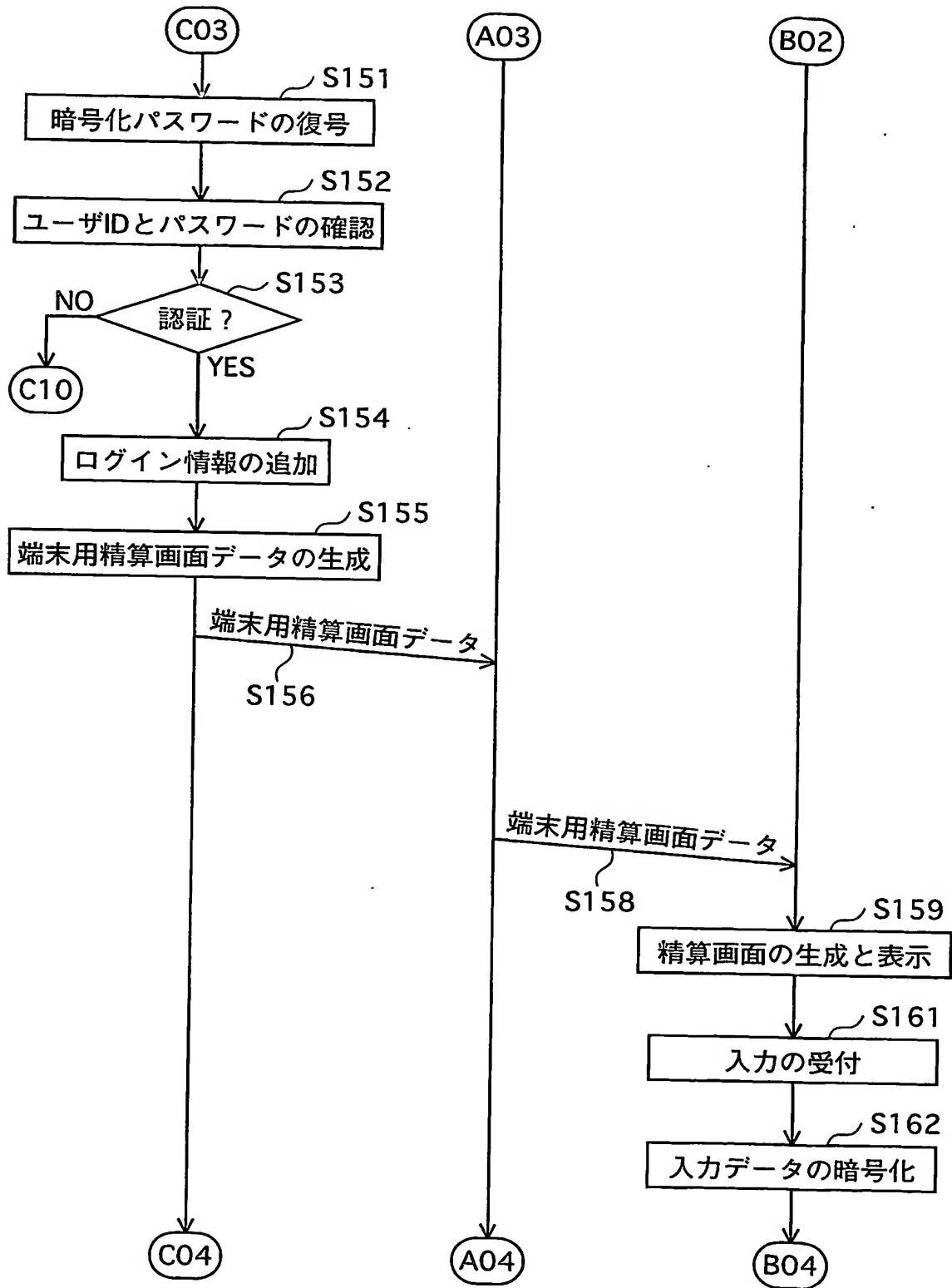


図24

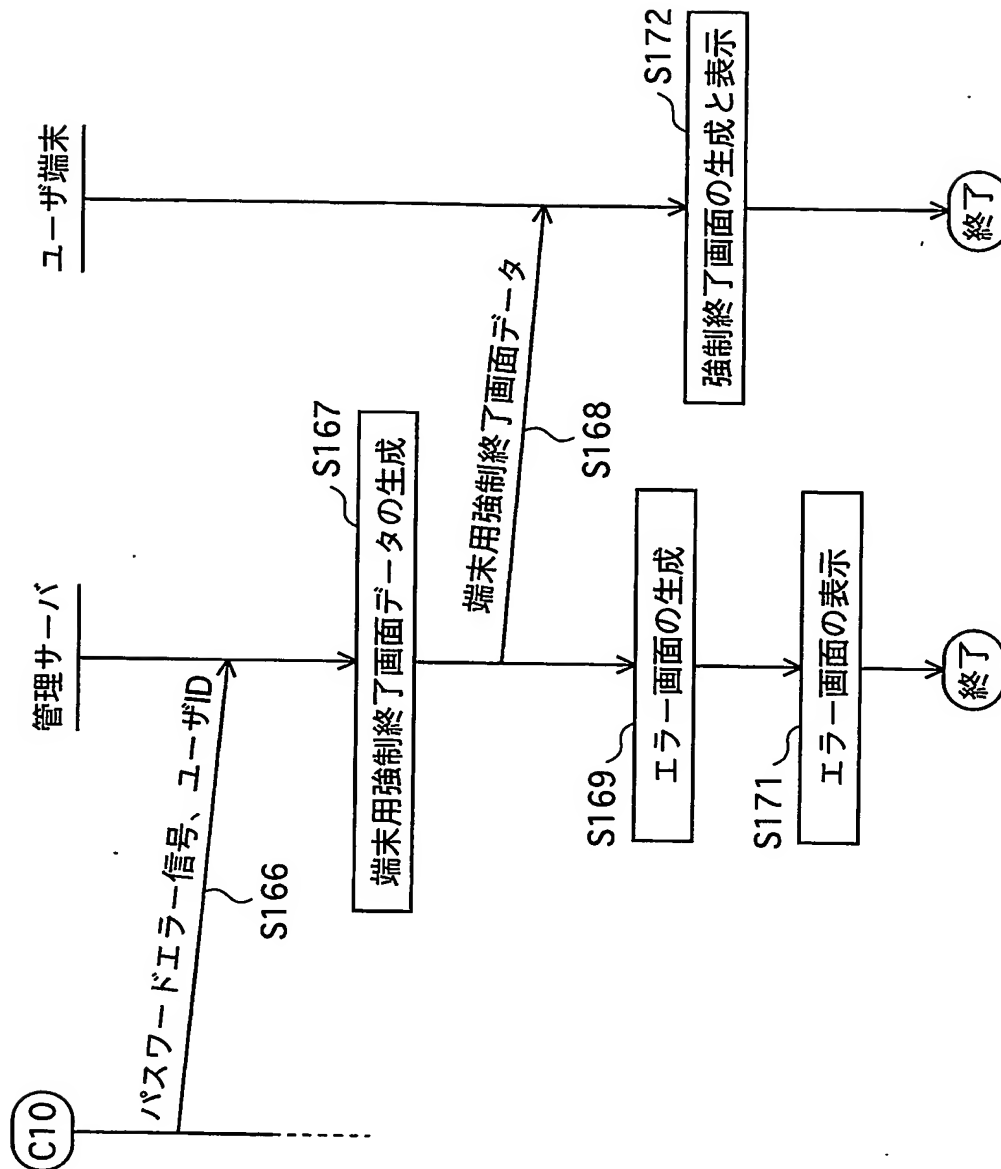


図25

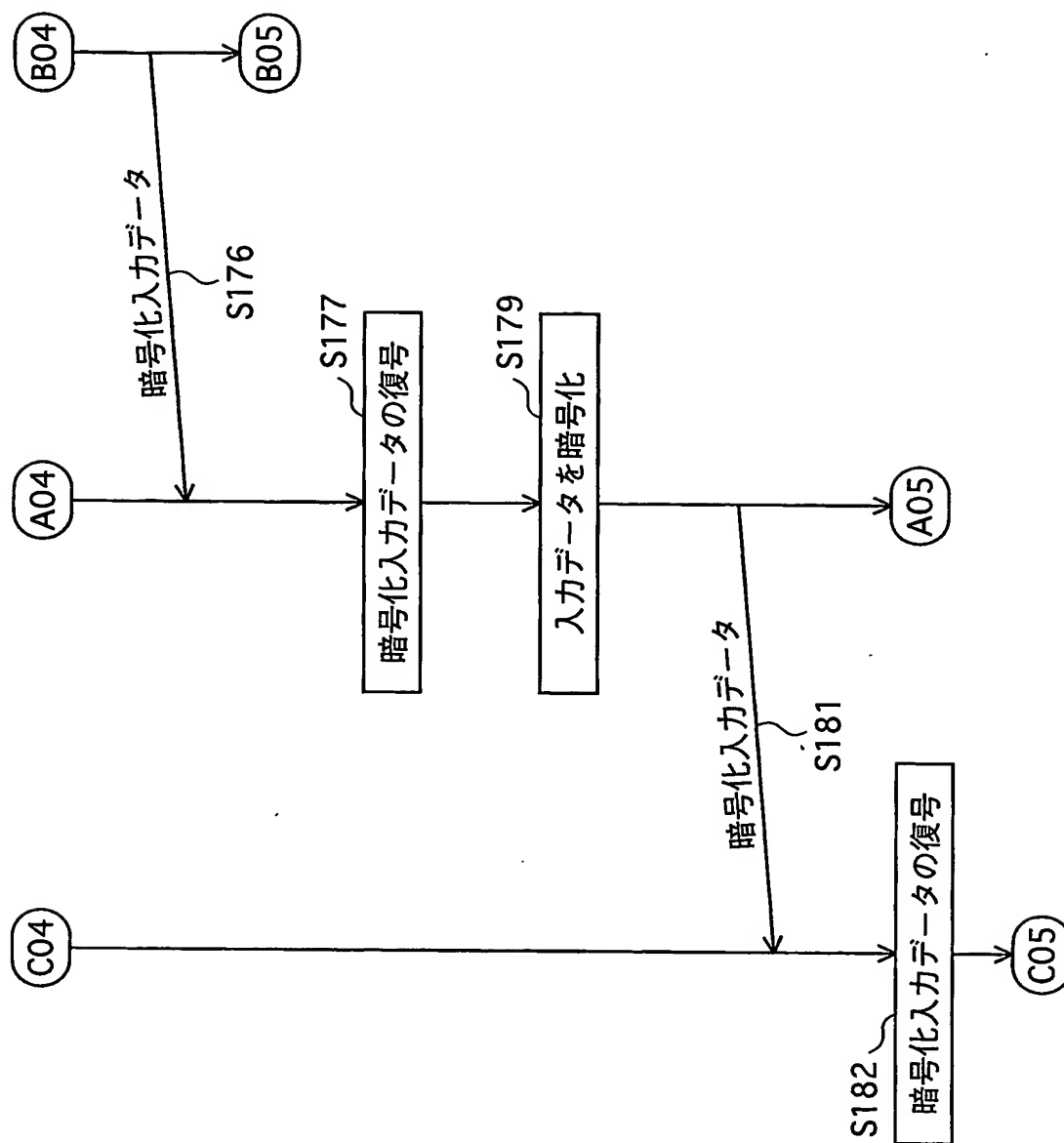


図26

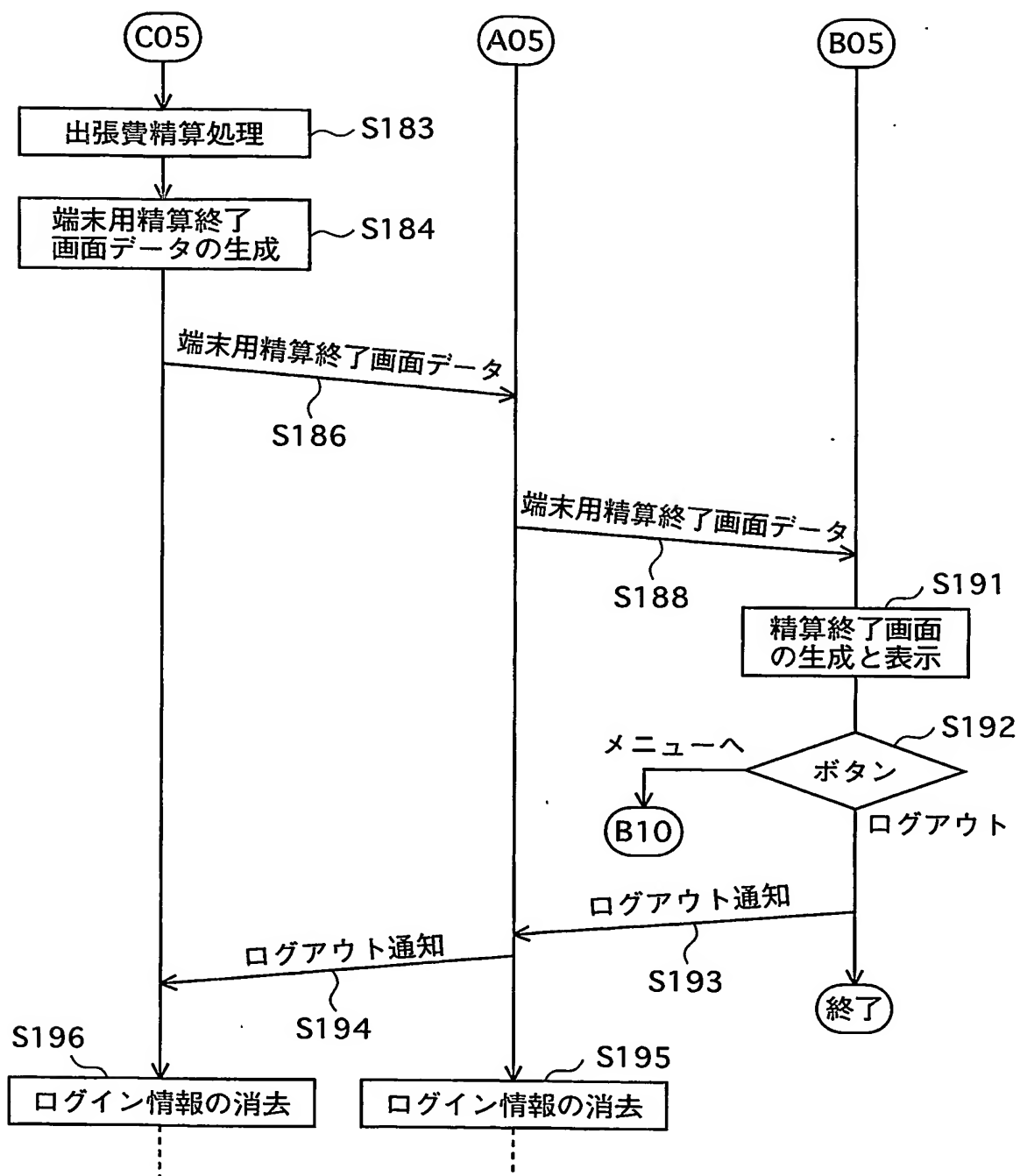


図27

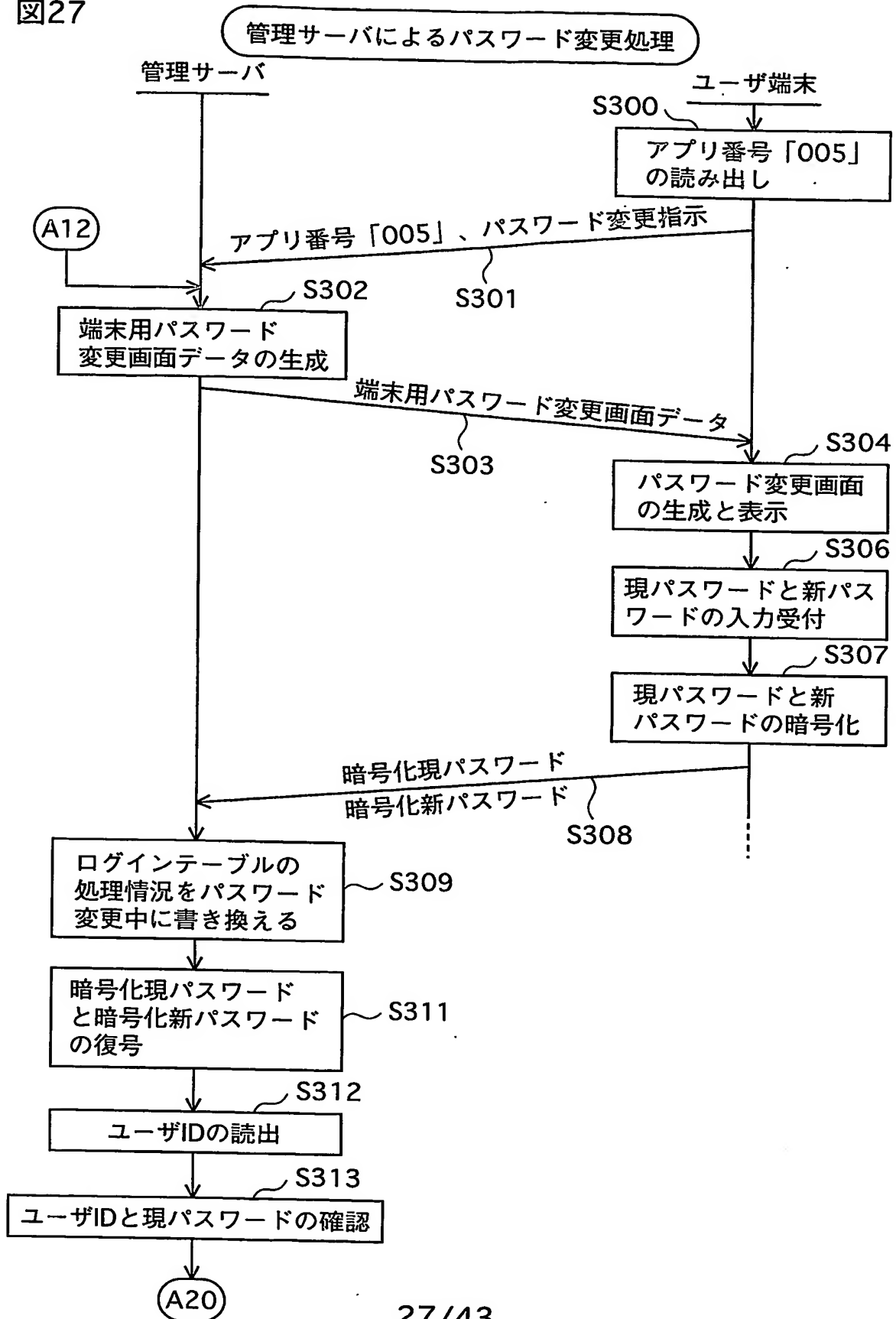


図28

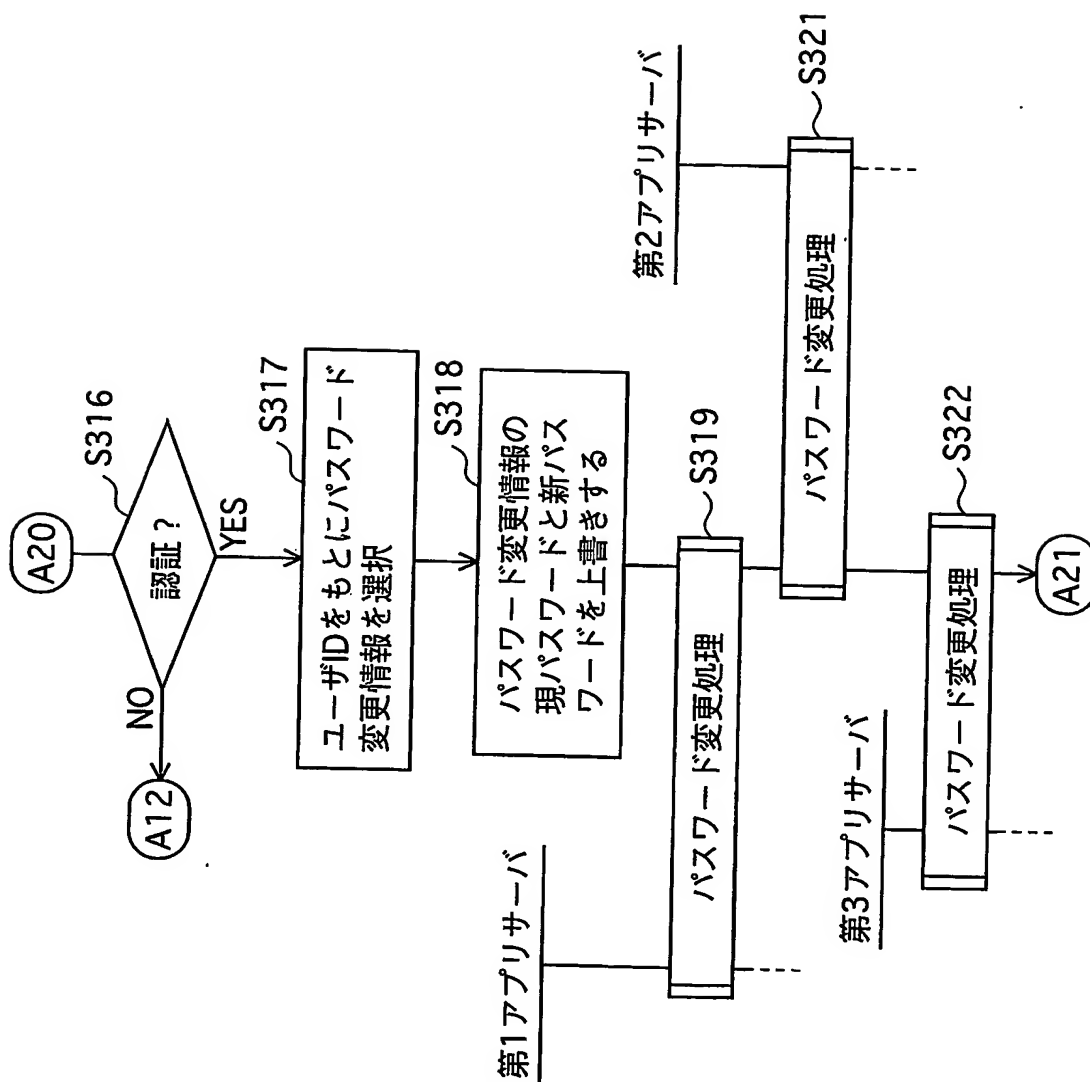


図29

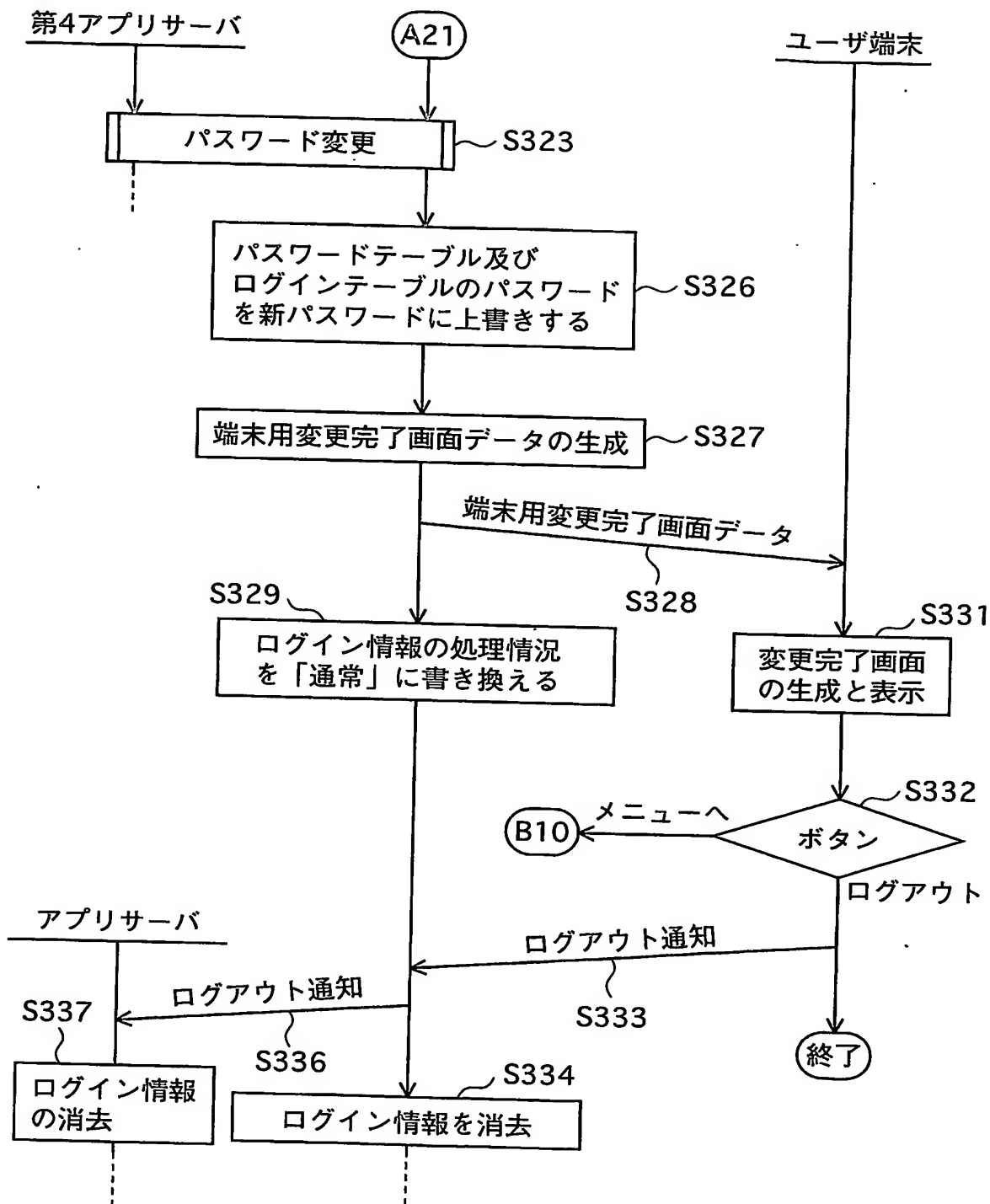


図30

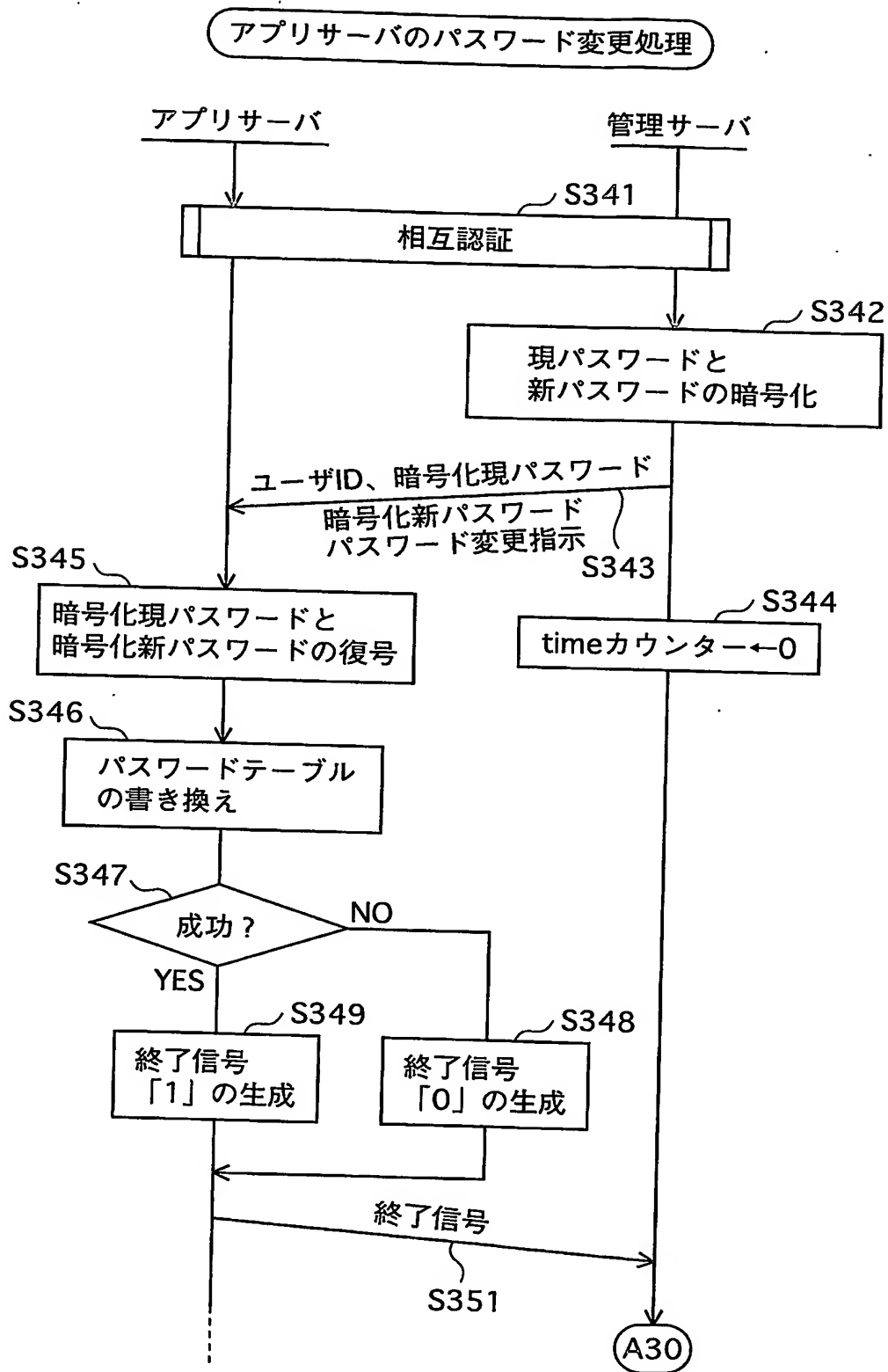


図31

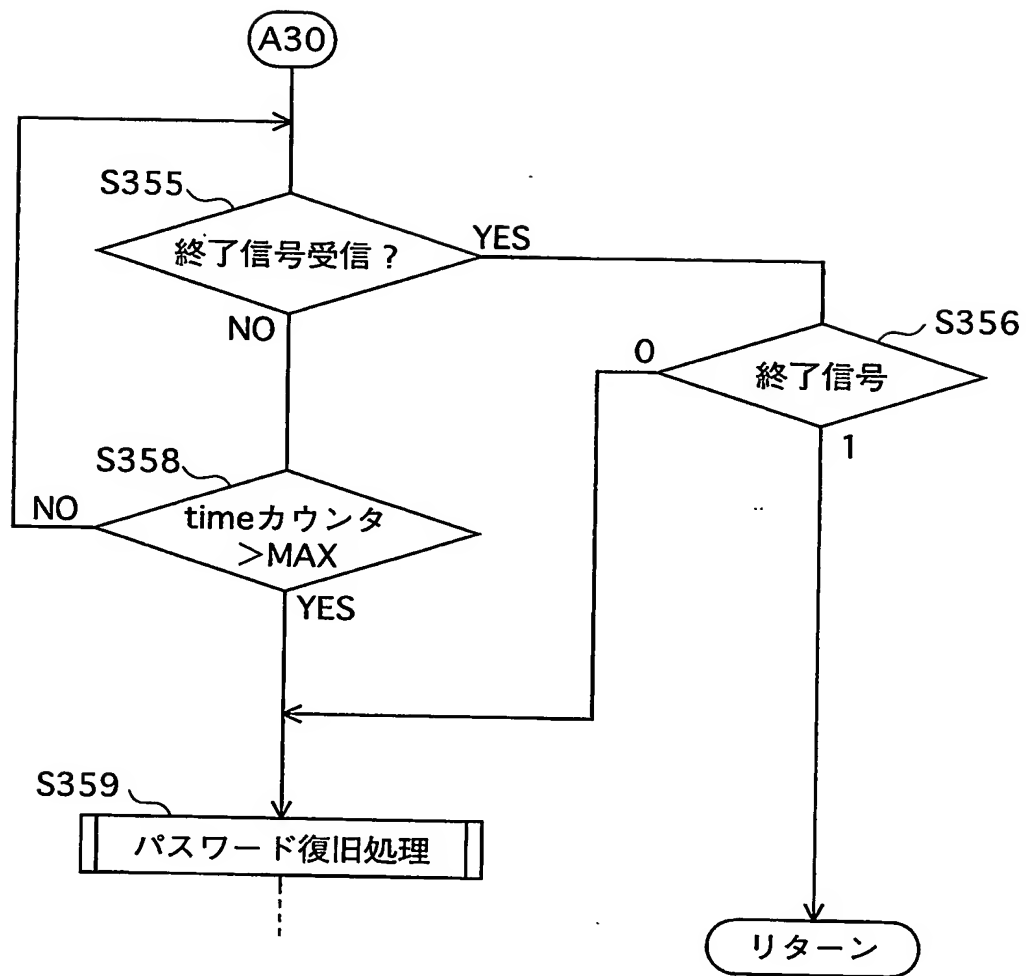


図32

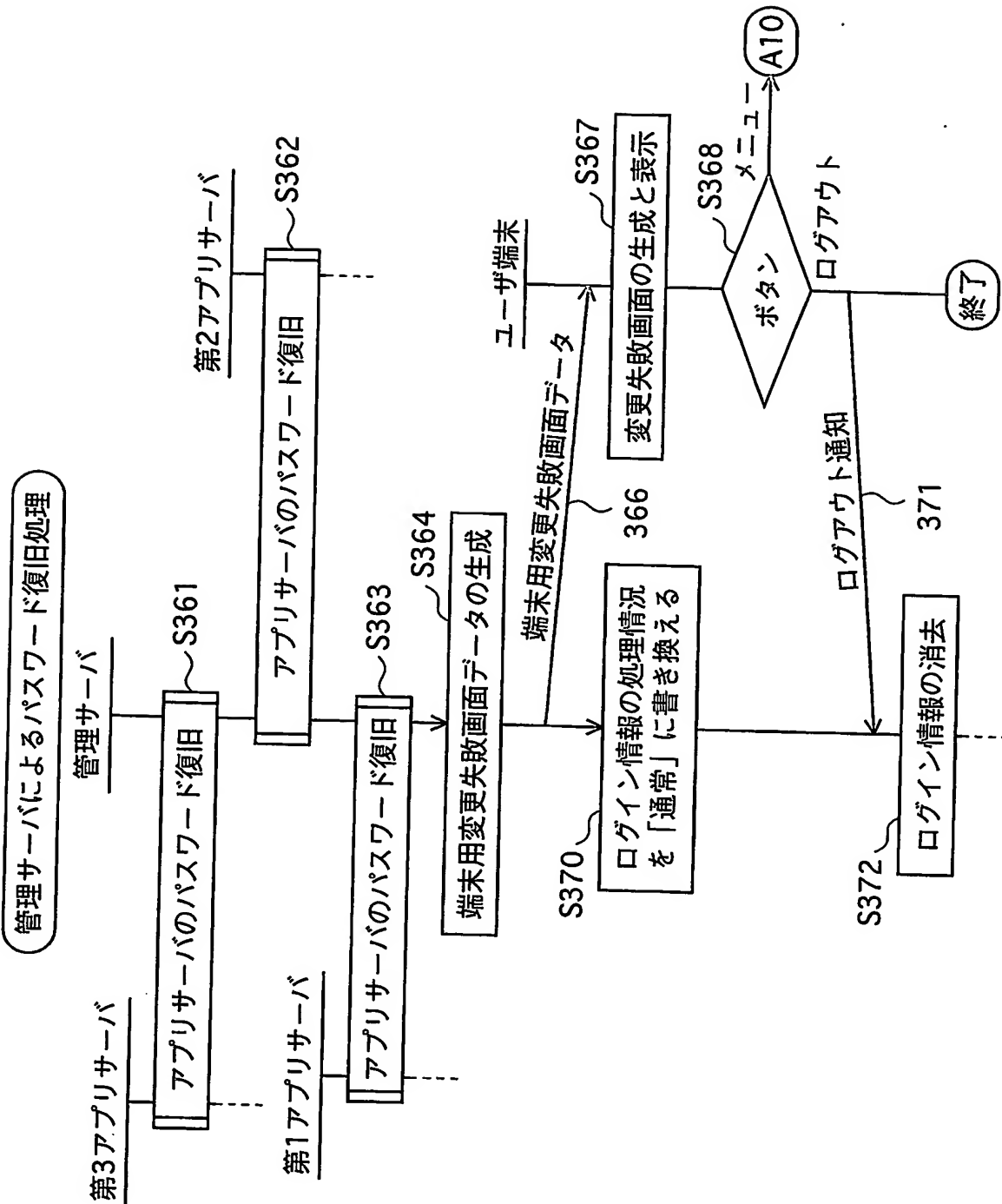


図33

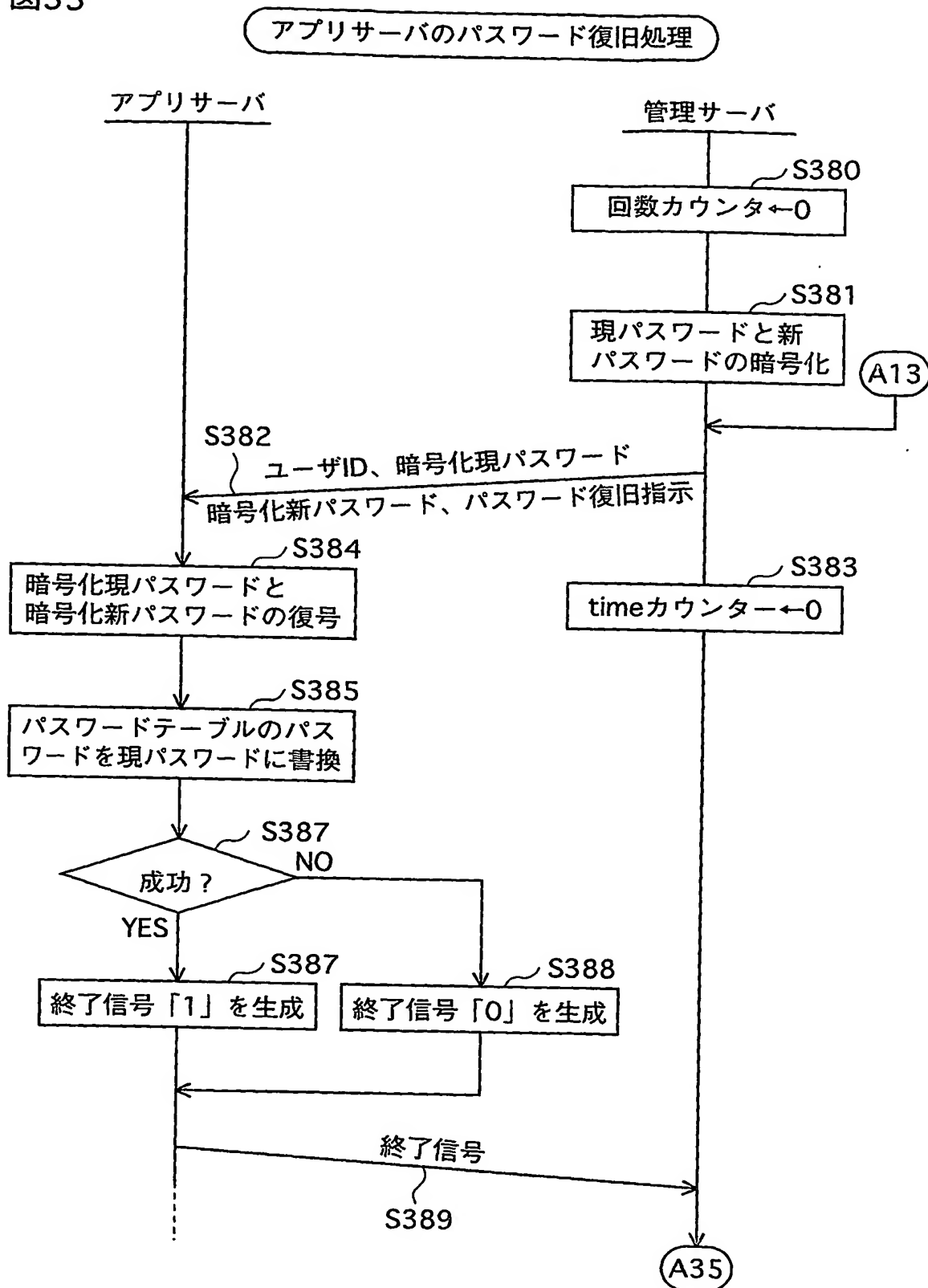


図34

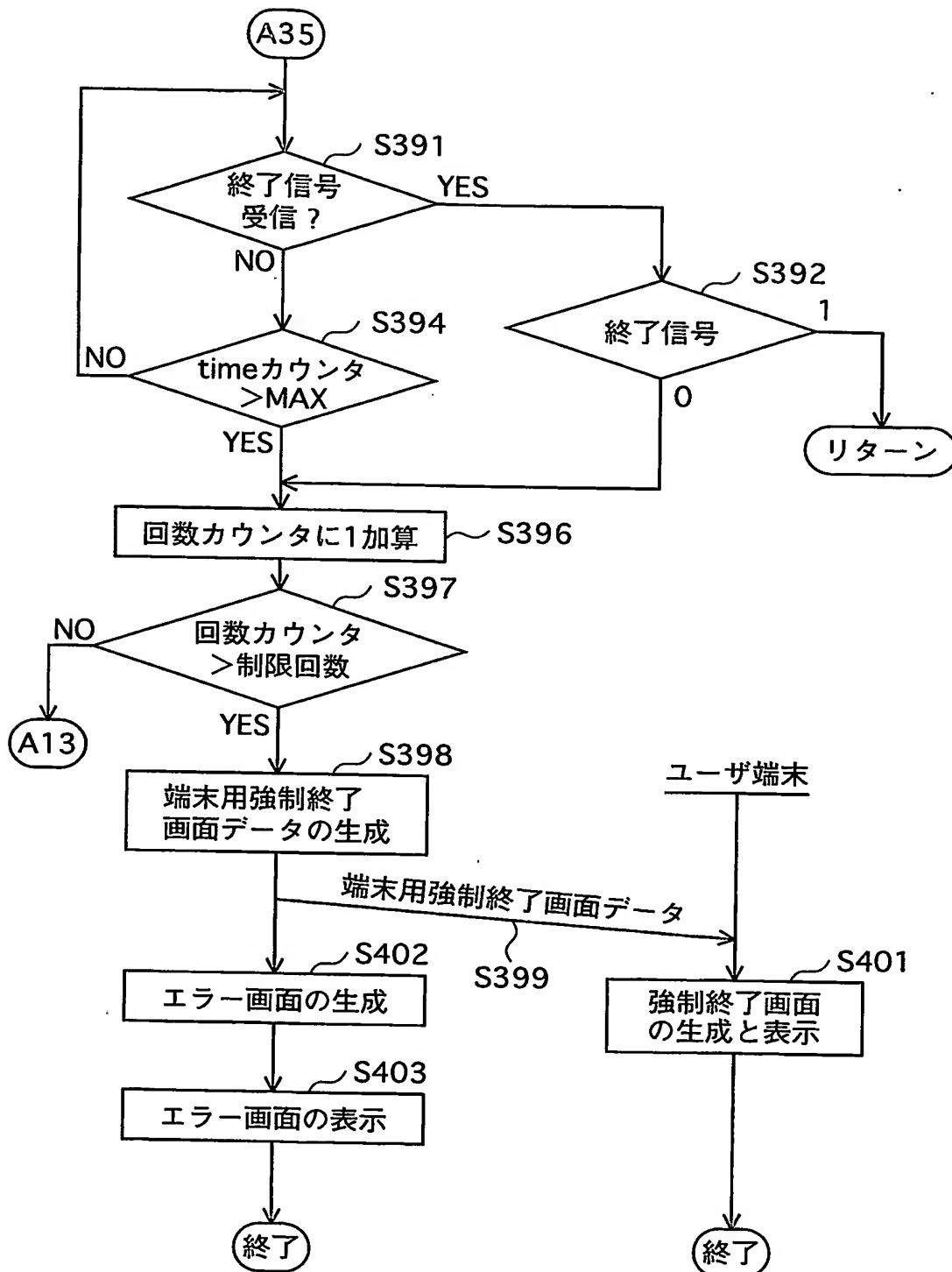


図35

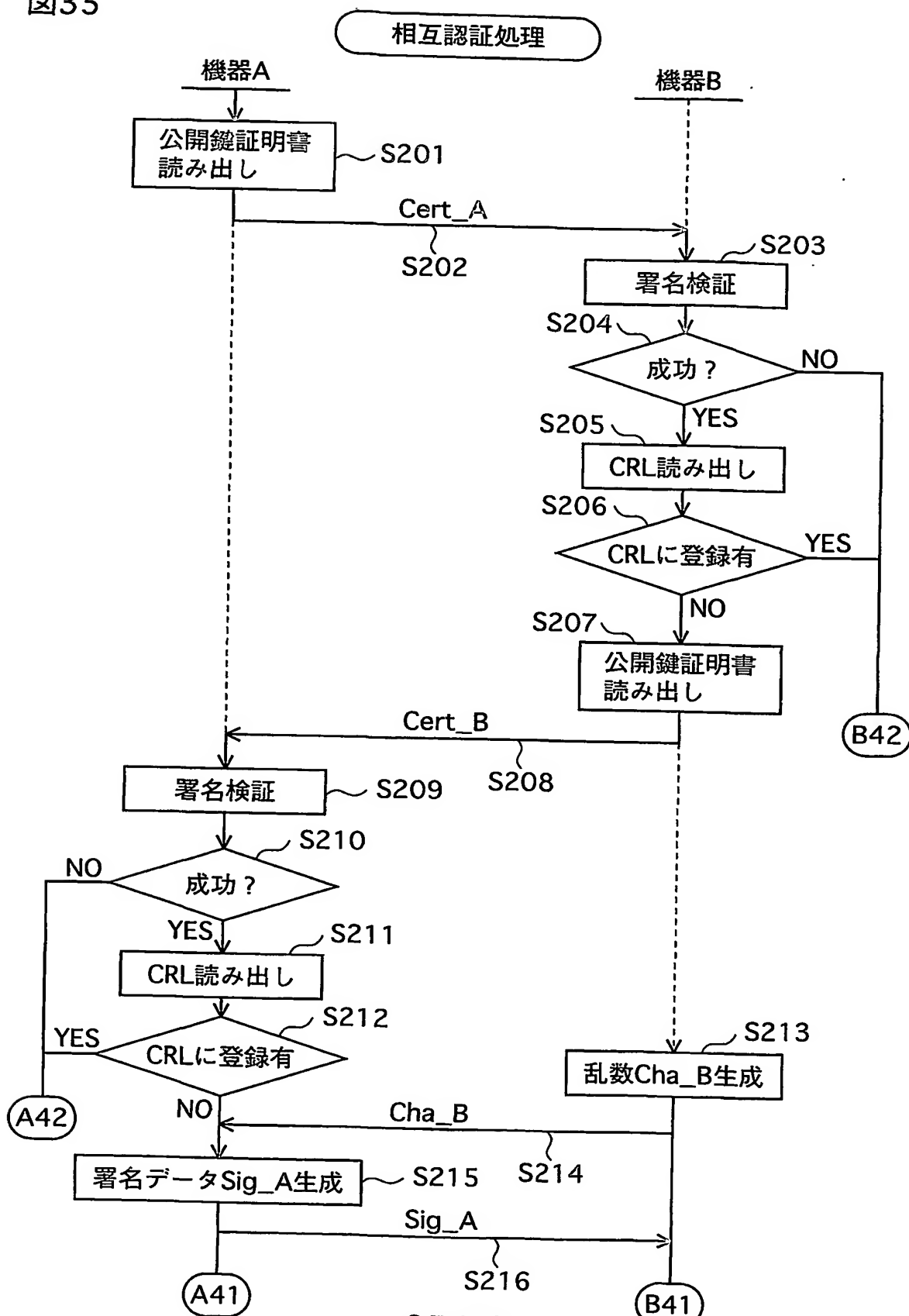


図36

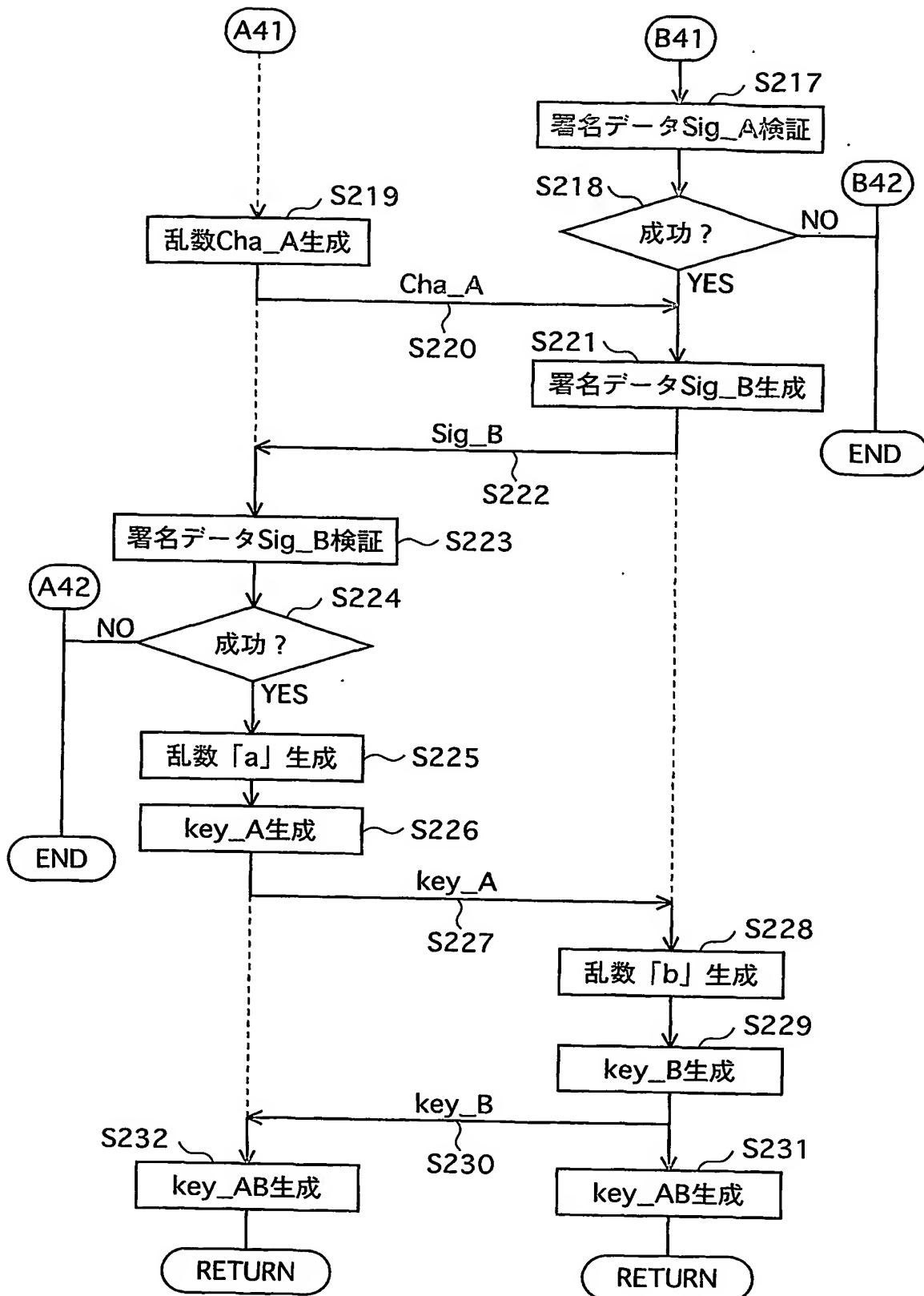


図37

(a)

アプリ サーバ名	第1 アプリサーバ	第2 アプリサーバ	第3 アプリサーバ	第4 アプリサーバ
パスワード	ozy12	ozy12	ozy12	ozy12

(b)

アプリ サーバ名	第1 アプリサーバ	第2 アプリサーバ	第3 アプリサーバ	第4 アプリサーバ
パスワード	nwy56	nwy56	ozy12	ozy12

(c)

アプリ サーバ名	第1 アプリサーバ	第2 アプリサーバ	第3 アプリサーバ	第4 アプリサーバ
パスワード	ozy12	ozy12	ozy12	ozy12

(d)

アプリ サーバ名	第1 アプリサーバ	第2 アプリサーバ	第3 アプリサーバ	第4 アプリサーバ
パスワード	nwy56	nwy56	nwy56	nwy56

図38

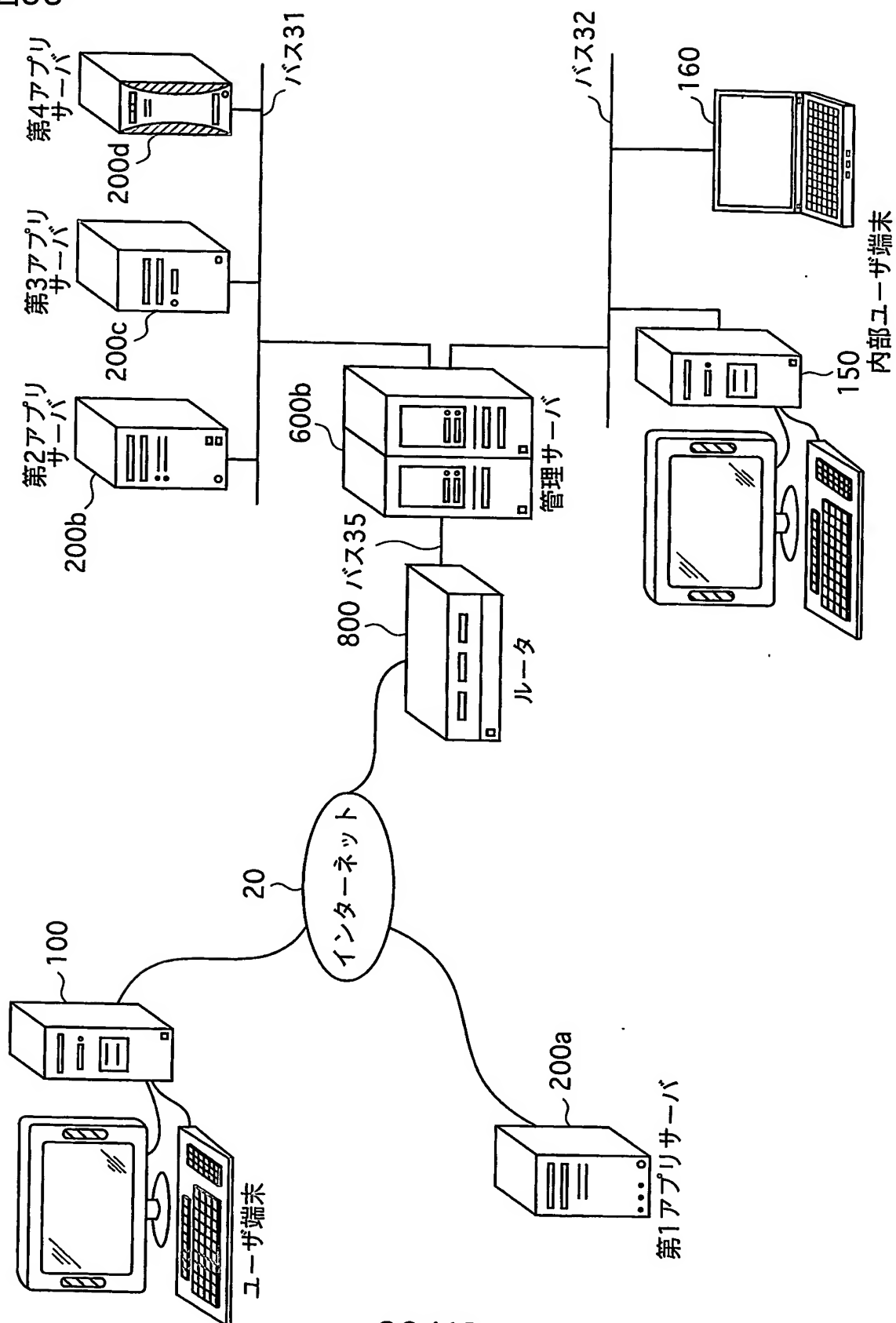


図39

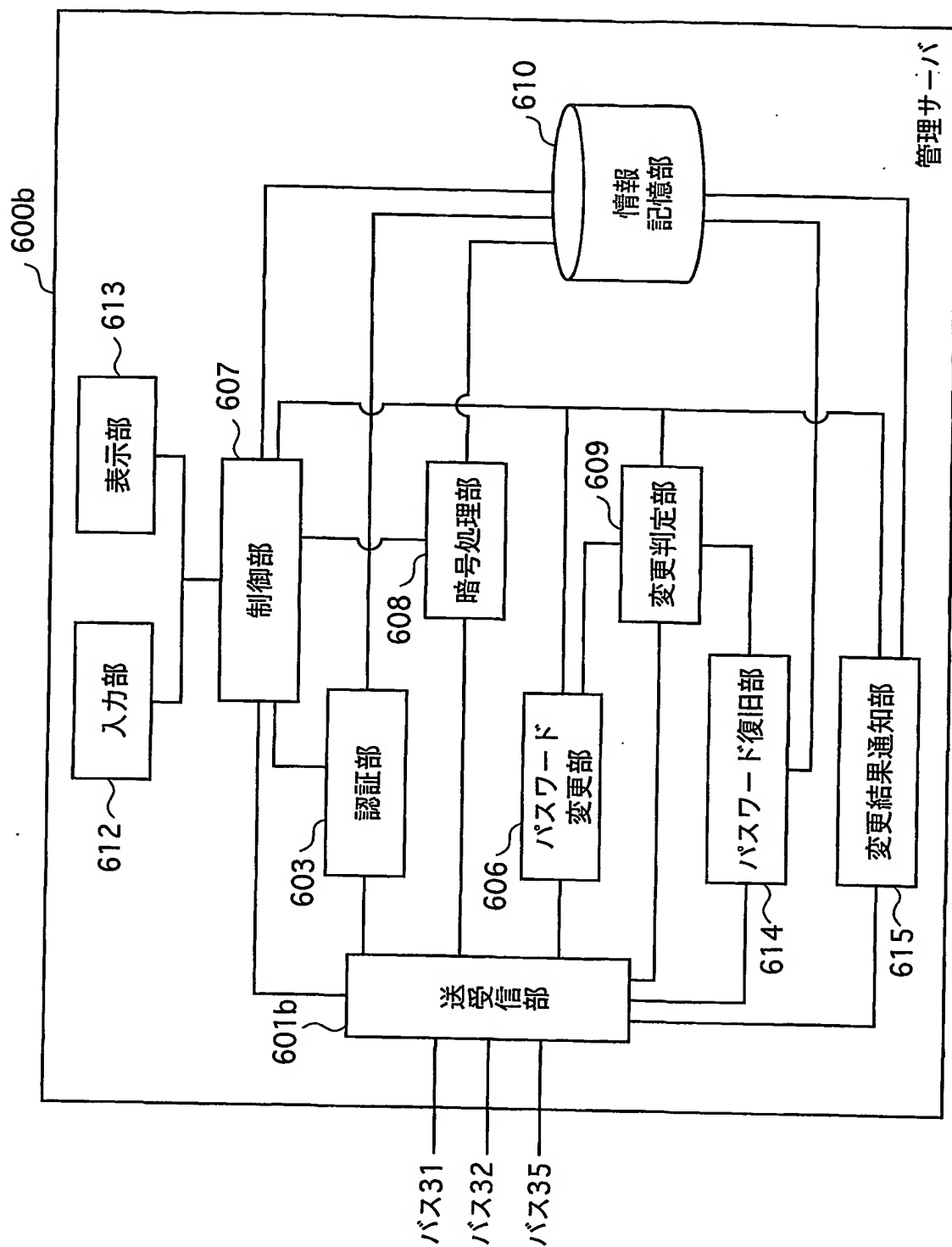


図40

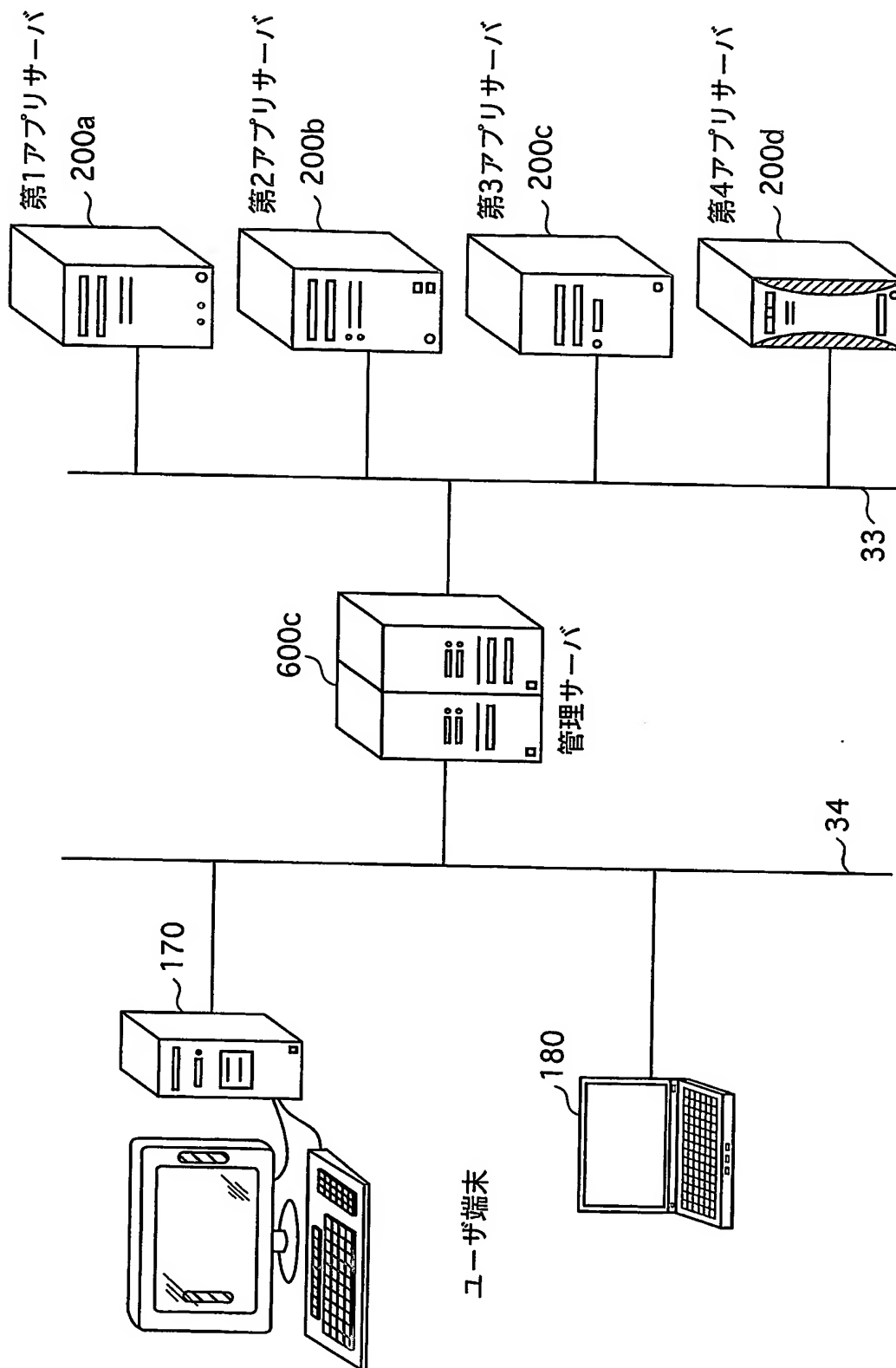


図41

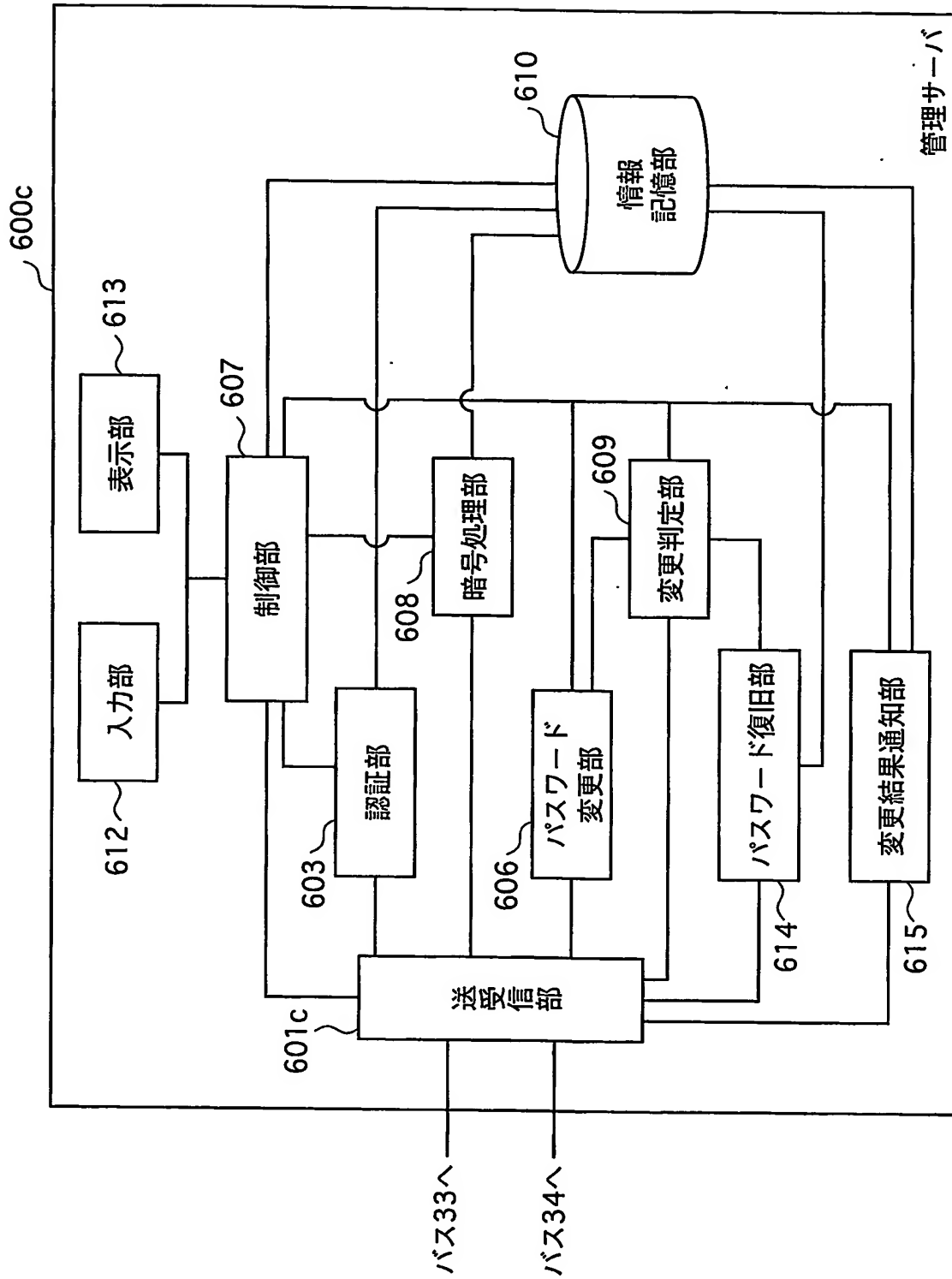


図42

パスワードテーブル

621b

ユーザID	氏名	パスワード	更新日
maeda	前田博子	ozy12	2003.05.10
nakamura	中村純一	klmoj	2003.04.28
suzuki	鈴木由香	spr01	2003.05.15
.	.	.	.
.	.	.	.
.	.	.	.

622b ~

623b ~

624b ~

図43

ルーティングテーブル

アプリ番号	ホスト名	IPアドレス	ポート番号	処理状況
001	system1	60.111.1.15	8000	通常
002	system2	60.111.1.20	8001	メンテナンス
・	・	・	・	・
・	・	・	・	・
・	・	・	・	・

642b ~

643b ~

・

・

・

641b

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/005205

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F15/00, H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F15/00, H04L9/32, G06F13/00, G06F1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST FILE (JOIS): Japanese
Computer Software Data Base (Japanese Patent Office): Japanese

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-043189 A (PFU Ltd.), 16 February, 2001 (16.02.01), Figs. 4 to 7 and their explanations (Family: none)	1-35
Y	Atsushi IIZAWA et al., "Database Omoshiro Koza", 1st edition, Kyoritsu Shuppan Co., Ltd., 30 April, 1993 (30.04.93), ISBN:4-320-02640-3, pages 189 to 210 (in particular, Fig. 10-4 in page 203)	1-35

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
10 May, 2004 (10.05.04)

Date of mailing of the international search report
25 May, 2004 (25.05.04)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/005205

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Philip A. Bernstein et al., translated by Kazuhiro OISO et al., "Transaction Shori System Nyumon", 1st edition, Nikkei Business Publications, Inc., 23 March, 1998 (23.03.98), ISBN:4-8222-8026-8, pages 13 to 16 and 256 to 279 (in particular, page 259, messages of "preparation request", "preparation completion" in Fig.9.1; page 262, messages of "preparation completion", "rejection" and descriptions concerning "time-out" on lines 12 to 16)	7-10
Y	JP 9-016502 A (Fujitsu Ltd.), 17 January, 1997 (17.01.97), Page 3, left column, pages 34 to 37 (Family: none)	12,13,22
Y	A.S. Tanenbaum, translated by Nobuyuki HIKICHI et al., "OS no Kiso to Oyo", 1st edition, Kabushiki Kaisha Toppan, 30 November, 1995 (30.11.95), ISBN:4-8101-8543-5, pages 460 to 462 (descriptions concerning name-server)	17
Y	Hirokazu NOBUKUNI et al., "Web to Mail de Seikyu Joho o Shokai Dekiru Web Billing", NTT Gijutsu Journal, 01 November, 2001 (01.11.01), ISSN:0915-2318, pages 94 to 97 (in particular, page 96, center column, line 15 to right column, line 1)	19

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G06F15/00, H04L9/32

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G06F15/00, H04L9/32, G06F13/00, G06F1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2004年
 日本国登録実用新案公報 1994-2004年
 日本国実用新案登録公報 1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JSTファイル (JOIS) : 日本語

Computer Software Data Base (日本国特許庁) : 日本語

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2001-043189 A (株式会社ピーエフユー) 2001.02.16, 図4-図7とその説明文 (ファミリーなし)	1-35
Y	飯沢篤志、外1名、データベースおもしろ講座、初版、共立出版株式会社、1993.04.30, ISBN:4-320-02640-3, pp. 189-210 (特に第203頁の図10-4)	1-35

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

10.05.2004

国際調査報告の発送日

25.5.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

久保 光宏

5B

9189

電話番号 03-3581-1101 内線 3546

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	フィリップ・A・バーンスタイン、外1名著、 大磯和広、外4名訳、トランザクション処理システム入門、初版、 日経BP社、1998.03.23, ISBN:4-8222-8026-8, pp. 13-16及び256-279 (特に第259頁の 図9.1の「準備要求」、「準備完了」メッセージと、 第262頁第12-16行の「準備完了」、「拒否」メッセージと 「時間切れ」に関する記述)	7-10
Y	JP 9-016502 A (富士通株式会社) 1997.01.17, 第3頁左欄第34-37行 (ファミリーなし)	12, 13, 22
Y	A. S. タネンバウム著、引地信之、外1名訳、 OSの基礎と応用、初版、株式会社トッパン、 1995.11.30, ISBN:4-8101-8543-5, pp. 460-462 (ネーム・サーバに関する記載)	17
Y	信國浩一、外3名、Webとメールで請求情報を照会できるWeb Billing, NTT技術ジャーナル, 2001.11.01, ISSN:0915-2318, pp. 94-97 (特に第96頁中央欄第15行 一同頁右欄第1行)	19